



Study on the use of Electronic Identification (eID) for the European Citizens' Initiative

Final Assessment Report

everis
September- 2017



an NTT DATA Company



EUROPEAN COMMISSION

*European Commission
B-1049 Brussels*

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information

TABLE OF CONTENTS

Table of Contents	3
List of Figures	6
List of Tables	8
Executive Summary	10
1 Introduction	15
1.1 European Citizens' Initiative	15
1.2 Objectives and scope	16
1.3 Structure of the study	19
2 Approach and methodology	20
2.1 Approach	20
2.2 Methods and techniques	23
3 Overview of the main components	26
3.1 The Online Collection System (OCS)	26
3.2 eID current state overview	28
3.3 eIDAS current state overview	36
4 Solution 1: Electronically signed PDF	38
4.1 Description	38
4.2 Legal analysis	41
4.3 Business analysis	44
4.4 Technical analysis	46
4.5 Assessment	47
5 Solution 2: Integration of e-signature	49
5.1 Description	49
5.2 Legal analysis	52
5.3 Business analysis	55
5.4 Technical analysis	56
5.5 Assessment	57
5.6 Comparison of solutions 1 and 2	58
6 Solution 3: Direct integration of eID	60
6.1 Description	60
6.2 Legal analysis	62
6.3 Business analysis	64
6.4 Technical analysis	65
6.5 Assessment	66

7	Solution 4: Integration with the eIDAS framework.....	68
7.1	Description	68
7.2	Legal analysis.....	70
7.3	Business analysis	74
7.4	Technical analysis	75
7.5	Assessment.....	76
7.6	Comparison of solutions 3 and 4.....	77
8	Solution 5: Prefilling user’s data with EU Login	79
8.1	Description	79
8.2	Data privacy overview	81
8.3	Business analysis	81
8.4	Technical analysis	82
8.5	Assessment.....	83
9	Solution 6: Prefilling user’s data with Facebook.....	85
9.1	Description	85
9.2	Data privacy overview	86
9.3	Business analysis	86
9.4	Technical analysis	90
9.5	Assessment.....	91
9.6	Comparison of solutions 5 and 6.....	91
10	Conclusions	93
11	References	96
12	Appendix A – Overview of the national eID schemes	98
13	Appendix B – Solution 1: Electronically signed PDF document.....	101
13.1	Detailed description	101
13.2	Overview of the legal framework.....	111
13.3	Business analysis	116
13.4	Technical analysis	120
14	Appendix C – Solution 2: e-signature	125
14.1	Detailed description	125
14.2	Overview of the legal framework.....	131
14.3	Business analysis	139
14.4	Technical analysis	142
15	Appendix D – Solution 3: Direct integration of eID	146
15.1	Detailed description	146

15.2	Overview of the legal framework.....	150
15.3	Business analysis	158
15.4	Technical analysis	163
16	Appendix E – Solution 4: Integration with the eIDAS Framework.....	167
16.1	Detailed description	167
16.2	Overview of the legal framework.....	171
16.3	Business analysis	180
16.4	Technical analysis	183
17	Appendix F – Solution 5: Prefilling user’s data with EU Login.....	187
17.1	Detailed description	187
17.2	Business analysis	188
17.3	Technical analysis	190
18	Appendix G – Solution 6: Prefilling user’s data with Facebook.....	192
18.1	Detailed description	192
18.2	Business analysis	193
18.3	Technical analysis	197
19	Appendix H – Evaluation Matrix.....	199
19.1	Evaluation Matrix – Solution 1	199
19.2	Evaluation Matrix – Solution 2	201
19.3	Evaluation Matrix – Solution 3	203
19.4	Evaluation Matrix – Solution 4	205
19.5	Evaluation Matrix – Solution 5	207
19.6	Evaluation Matrix – Solution 6	208
20	Appendix I – Terms and acronyms.....	209
20.1	Acronyms used throughout the report	209
20.2	Glossary	210

LIST OF FIGURES

Figure 1: The ECI process.....	15
Figure 2: The three layers of the analysis.....	17
Figure 3: Breakdown of solution analysis.....	18
Figure 4: Sequence of the processes.....	19
Figure 5: Approach	20
Figure 6: Components of the study.....	21
Figure 7: Evaluation Matrix	23
Figure 8: SWOT analysis	24
Figure 9: Challenges and opportunities	26
Figure 10: Process of authentication with certificates.....	31
Figure 11: Different flows of information that include the use of e-signature.....	39
Figure 12: Architecture of electronically signed PDF document - collection phase	40
Figure 13: Assessment of solution 1.....	48
Figure 14: Architecture and dataflows for e-signature	49
Figure 15: Assessment of solution 2.....	58
Figure 16: SWOT analysis of solutions 1 and 2.....	58
Figure 17: Architecture and dataflows for direct integration of eID.....	60
Figure 18: Assessment of solution 3.....	67
Figure 19: Architecture and dataflows of eIDAS integration	69
Figure 20: Assessment of solution 4.....	77
Figure 21: SWOT analysis of solutions 3 and 4.....	77
Figure 22: Architecture and dataflows for EU Login	80
Figure 23: Summary of the business analysis – EU Login.....	82
Figure 24: Assessment of solution 5 – EU Login.....	84
Figure 25: Architecture and dataflows for Facebook.....	85
Figure 26: Assessment of solution 6 – Facebook	91
Figure 27: SWOT analysis of solutions 5 and 6.....	92
Figure 28: Overview of the national eID schemes	100
Figure 29: Description of the actions for the collection of statements of support	102
Figure 30: Use case: electronically signed PDF document - collection phase.....	104
Figure 31: Activity diagram of the collection process	105
Figure 32: Description of the actions for the collection of statements of support	107
Figure 33: Use case: electronically signed PDF document - verification phase	108
Figure 34: Activity diagram of the verification process.....	109
Figure 35: Responses from Member States. Question 1.....	114
Figure 36: Responses from Member States. Question 2.....	115
Figure 37: Responses from Member States. Question 3.....	116
Figure 38: Activity diagram of the collection process – part 1.....	127
Figure 39: Activity diagram of the collection process – part 2.....	130
Figure 40: Responses from Member States. Question 1.....	136
Figure 41: Responses from Member States. Question 2.....	137
Figure 42: Responses from Member States. Question 3.....	138
Figure 43: Responses from Member States. Question 4.....	138
Figure 44: Activity diagram of the collection process	150

Figure 45: Responses from Member States. Question 1..... 155
Figure 46: Responses from Member States. Question 2..... 156
Figure 47: Responses from Member States. Question 3..... 156
Figure 48: Responses from Member States. Question 4..... 157
Figure 49: Responses from Member States. Question 5..... 158
Figure 50: Responses from Member States. Question 6..... 162
Figure 51: Activity diagram of the collection process - part 1 171
Figure 52: Activity diagram of the collection process - part 2 171
Figure 53: Responses from Member States. Question 7..... 178
Figure 54: Responses from Member States. Question 8..... 179
Figure 55: Responses from Member States. Question 9..... 179
Figure 56: Responses from Member States. Question 8(2) 181
Figure 57: Activity diagram of the collection process 188
Figure 58: Activity diagram of the collection process 193

LIST OF TABLES

Table 1: Summary of the changes required to ECI and Implementing Regulation	10
Table 2: Comparison of solutions 1 and 2	12
Table 3: Comparison of solutions 3 and 4	13
Table 4: Comparison of solutions 5 and 6	14
Table 5: Description of the evaluation criteria.....	25
Table 6: Overview of the eID available data	35
Table 7: Overview of the eIDAS datasets and ECI personal data requirements	37
Table 8: Legal analysis: ECI Regulation - solution 1.....	42
Table 9: Comparison of e-signature standards, eIDAS Regulation - solution 1.....	43
Table 10: Summary of the business analysis - e-signed PDF document	46
Table 11: Summary of the technical analysis - e-signed PDF document.....	47
Table 12: Legal analysis: ECI Regulation - solution 2.....	52
Table 13: Legal analysis, eIDAS Regulation - solution 2	53
Table 14: Summary of the business analysis - e-signature	56
Table 15: Summary of the technical analysis - e-signature.....	57
Table 16: Comparison of solutions 1 and 2	59
Table 17: Legal analysis: ECI Regulation - solution 3.....	62
Table 18: Summary of the business analysis – Direct integration of eID.....	65
Table 19: Summary of the technical analysis – Direct integration of eID	66
Table 20: Legal analysis: ECI Regulation - solution 4.....	71
Table 21: Legal analysis: eIDAS Regulation - solution 4	73
Table 22: Summary of the business analysis – Integration with the eIDAS framework	75
Table 23: Summary of the technical analysis – Integration with the eIDAS framework.....	76
Table 24: Comparison of solutions 3 and 4	78
Table 25: Summary of the technical analysis – EU Login	83
Table 26: Comparison of the personal data requirements and the data stored in Facebook	88
Table 27: Summary of the business analysis – Facebook.....	89
Table 28: Summary of the technical analysis – Facebook.....	90
Table 29: Comparison of solutions 5 and 6	92
Table 30: Summary of the changes required to ECI and Implementing Regulation	93
Table 31: Actors for the collection of statements of support	104
Table 32: Actors for the verification of statements of support	108
Table 33: Description of the actions for the verification of statements of support	110
Table 34: Legal analysis, ECI Regulation - solution 1.....	113
Table 35: Use case - integration of e-signature	126
Table 36: Actors for collection of statements of support	126
Table 37: Legal analysis, ECI Regulation - solution 2.....	133
Table 38: Legal analysis, eIDAS Regulation - solution 2	135
Table 39: Description of the actions for the collection of statements of support.....	148
Table 40: Use case - direct integration of eID	149
Table 41: Actors for collection of statements of support	149
Table 42: Legal analysis, ECI Regulation - solution 3.....	153
Table 43 : Description of the actions for the collection of statements of support.....	168
Table 44: Use case - indirect integration of eID connecting to eIDAS network.....	170

Table 45: Actors for the collection of statements of support	170
Table 46: Legal analysis, ECI Regulation - solution 4.....	174
Table 47: Legal analysis, eIDAS Regulation - solution 4	177
Table 48: Use case - EU Login	187
Table 49: Actors for collection of statements of support	188
Table 50: Use case - Facebook	192
Table 51: Actors for collection of statements of support	193
Table 52: Comparison between the ECI personal data requirements and the data stored in Facebook accounts	196
Table 53: Acronyms	209
Table 54: Glossary	210

EXECUTIVE SUMMARY

In the context of the European Citizen's Initiative, everis received the mandate to explore the use of Electronic Identification (eID) for the European Citizen's Initiative. For such purpose, a thorough research on the existing solutions and previous studies has been carried out, and Member States were consulted through questionnaires. Departing from the ground work presented in the Assessment of ICT impacts of the Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative study published in 2015¹, everis identified several suitable solutions that can be divided into three main categories:

- Solutions considering the use of electronic signatures:
 - Solution 1 foresees the submission of statements of support through an electronically signed PDF that the user uploads to the Online Collection System (OCS).
 - Solution 2 comprises a direct integration of e-signature solutions into the OCS, allowing citizens to sign statements of support online.
- Solutions based on electronic identification:
 - Solution 3 provides a direct integration of national eID into the OCS in order to allow citizens to authenticate themselves and support initiatives online.
 - Solution 4 also provides an integration of eID through the eIDAS framework.
- Complementary solutions, aiming at easing the submission process and attracting more users to the ECI tool:
 - Solution 5 could allow EU Login users (formerly ECAS) to pre-fill the data fields with the data stored in their accounts.
 - Solution 6 foresees a connection with a social network, namely Facebook, by which users would pre-fill the data requirements.

From a legal point of view, several changes, both to the ECI and to the Implementing Regulation, are necessary for the implementation of the different solutions. Those changes are summarised in the following table. More information can be found in the legal analysis of the respective solutions.

Solution	Change Required		Description
	ECI Regulation	Implementing Regulation	
1	(Yes)	Yes	Annex III Re-wording of Article 5.2 is advisable but not mandatory
2	Yes	Yes	Article 8 and Annex III Re-wording of Article 5.2 is advisable but not mandatory
3	Yes	Yes	Articles 5 & 8 and Annex III
4	Yes	Yes	Articles 5 & 8 and Annex III
5	No	No	n/a
6	No	No	n/a

Table 1: Summary of the changes required to ECI and Implementing Regulation

¹ European Commission (2015) *Assessment of ICT impacts of the Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative*.

SOLUTION 1: PDF document

Solution 1 considers the use of a PDF document that citizens could download from the OCS, sign electronically in their local computer or device, and upload back to the system. The OCS would store the signed statements of support that would be sent for verification once the collection phase comes to an end. The ECI Regulation already foresees the possibility of using an electronic signature for supporting an initiative. Therefore, only Annexes III and V should be modified to include a more specific mention to the use of such method to submit a statement of support. Moreover, a rewording of Article 5, updating the reference to the use of advanced electronic signature to qualified electronic signature is advisable.

The main advantage of this solution relies on the expected smooth implementation, as this solution does not require major changes in the OCS, and no direct connection with e-signature access points from Member States are needed. Furthermore, verifying authorities are proposed to check the validity of the certificate only when the statement of support is submitted, simplifying their current tasks. According to the information provided by Member States, e-signature seems to be at a suitable maturity level for interface with the OCS.

On the other hand, the main drawback of this solution is that it might negatively impact the user experience, as it requires additional steps to be completed.

SOLUTION 2: Integration of e-signature

In contrast with the previous alternative, this solution could allow users to access the system and use their e-signature online in the OCS. The Digital Signature Services (DSS) provided under eSignature CEF Building Block is used to establish a connection with the corresponding Member State's e-signature services, allowing users to authenticate themselves and retrieve data from their certificates. Such data shall be stored with an indicator that accounts for validated information, which would, in theory, not require further verification from the competent authorities. If this implementation path is finally not agreed on, another alternative would be to store the certificates and send them for validation at the end of the collection phase.

Contrary to solution 1, this solution provides, as main advantages, to allow for an automatic validation of the statement of support, and to create a smooth and fast procedure for users to support an initiative. These changes in the system would require a specific modification of Article 8, as a new procedure for the validation needs to be established. Consequently, the data requirements of Annex III might be also modified. In addition, a similar change in Article 5 of the Regulation than in solution 1 (specific mention to qualified certificates) is advisable.

This solution presents the advantages of allowing the online validation of the e-signature and of limiting the implementation costs, as it reuses an IT solution that hides the complexity of the interactions with the national e-signature solution.

As solution 1 and 2 can easily be compared, the table hereunder provides an overview of the results based on a set of the identified evaluation criteria.

Evaluation Criteria	Solution 1	Solution 2	
ECI Regulation	● ● ● ● ● ●	● ● ● ● ● ●	Solution 2 requires an amendment of Article 8 and a modification of Annex III while no change in the regulation is necessary for the implementation of solution 1.
eIDAS Regulation	● ● ● ● ● ●	● ● ● ● ● ●	Both solutions comply with the eIDAS Regulation
Member States' responses	● ● ● ● ● ●	● ● ● ● ● ●	The comparison of the responses is not relevant as the questions focused on different aspects of each solution.
Ease of use	● ● ● ● ● ●	● ● ● ● ● ●	Compared to solution 1, the data retrieved from e-signature is trustful and the validation task is therefore easier. Moreover, the process for the citizens is smooth and user-friendly.
Quantity of data	● ● ● ● ● ●	● ● ● ● ● ●	By implementing solution 2, the quantity of data to be inserted by the user is reduced to zero and the number of statements of support to be validated by verification authorities is reduced while for solution 1, they still need to verify the identity of signatories.
Penetration	● ● ● ● ● ●	● ● ● ● ● ●	Only 50% of the Member States consulted can assure that eSignature is issued to the majority of adult population. However, for both solutions, the data is retrieved from trustworthy sources, easing the task of verification authorities
Operational aspects	● ● ● ● ● ●	● ● ● ● ● ●	The two solution are mainly similar regarding operational aspects
Security	● ● ● ● ● ●	● ● ● ● ● ●	The two solutions are mainly similar regarding security
Integration	● ● ● ● ● ●	● ● ● ● ● ●	Solution 2 is more complex to integrate than solution 1

Table 2: Comparison of solutions 1 and 2

SOLUTION 3: Direct integration with national eID

This solution is based on the use of eID in order to establish a connection with the eID access points of the different Member States, by which users could authenticate themselves and support the selected initiative. Similarly to solutions 2 and 4, a first option would consist in storing the data with an indicator that accounts for the statements of support submitted via eID. Given the fact that the user's data would be coming from a trustworthy source, no additional validation would need to be performed. The Regulation might need to be adapted to provide a sound legal ground when implementing this solution. A specific reference to the use of eID might need to be included in Article 5. Besides, Article 8 may need to be modified as well, to account for a new procedure to validate the statements of support when they are submitted. Annex III should also be modified accordingly.

The fact that citizens could go through a fast and user-friendly process and that statements of support would be validated on the spot when users authenticate themselves are the main added values of this solution.

However, the complex technical implementation of this solution is seen as one of the main drawbacks and is the main reason for the creation of eIDAS in the first place. Indeed, at least one specific module per Member State needs to be integrated into the OCS. In addition, at the moment of writing this report, not all Member States have implemented compatible eID schemes, although according to the responses received, in many cases, eID is issued to a majority of the adult population in countries where it is implemented.

SOLUTION 4: Integration with eIDAS

Solution 4 is similar to the previous one, as it is also based on eID, although the connection between the OCS and the Member States would be established through the eIDAS network. Given the similarity of both eID solutions, the required legal changes are equivalent. However, in this case, a specific mention to the use of the eIDAS network is advisable. It is important to mention that solutions 3 and 4 are not exclusive, as the integration through eIDAS could be activated for the Member States whose eIDAS node is ready, while direct integration with national eIDs could be

implemented temporarily for the other countries, while they achieve a successful implementation of their eIDAS node.

This solution would also bring an added value regarding user-friendliness of the OCS and on-the-spot validation. Furthermore, given the eIDAS architecture, implementation efforts would be much lower than in solution 3, as it requires an integration with a single eIDAS node in order to interact with any national eID scheme already available through eIDAS.

Although this solution is very promising, it should be noted that the eIDAS network is still under implementation in most Member States. At the moment of writing this report, only three eID schemes (Germany, Austria and the Netherlands) have interconnected their nodes, and Spain is the only country that has successfully completed the EC acceptance tests.

As solution 3 and 4 can be easily compared, the table hereunder provides an overview of the results based on a set of the identified evaluation criteria.

Evaluation Criteria	Solution 3	Solution 4	
ECI Regulation	● ● ● ● ○	● ● ● ● ○	In addition to the changes necessary for both solutions, solution 4 also requires a specific mention to the eIDAS Regulation.
eIDAS Regulation	n/a	● ● ● ● ●	This criterion is not applicable for solution 3. The implementation of solution 4 falls within the scope and is compliant with the eIDAS Regulation.
Member States' responses	● ● ● ● ● ○	● ● ● ● ● ○	The comparison of the responses is not relevant as the questions focused on different aspects of each solution.
Ease of use	● ● ● ● ● ○	● ● ● ● ● ○	Regarding the ease of use, the direct integration of eID and the integration with the eIDAS framework are similar.
Quantity of data	● ● ● ● ● ○	● ● ● ● ● ○	The quantity of data is comparable for both solutions.
Penetration	● ● ● ● ● ○	● ● ● ● ● ○	The penetration level of both solutions is similar. However, some eIDAS nodes are still in preproduction phase and will be fully operational by 2018.
Operational aspects	● ● ● ● ● ○	● ● ● ● ● ○	While the scalability and maintainability of solution 4 should not cause any problem, a lot of changes and effort are required regarding solution 3.
Security	● ● ● ● ● ○	● ● ● ● ● ○	For solution 4, the attribute of the SAML response "InReplyTo" must have the same value as the ID of the request. This is the only slight difference between solutions 3 and 4 regarding security.
Integration	● ● ● ● ● ○	● ● ● ● ● ○	The integration of solution 3 is more complex than solution 4. Regarding the maturity, solution 3 is more advanced than the eIDAS framework integration. In addition, even though the two solutions are similar from a portability point of view, solution 3 requires more costs and efforts to be implemented.

Table 3: Comparison of solutions 3 and 4

COMPLEMENTARY SOLUTIONS

The scope under which solutions 5 and 6 might operate is different than the previous ones, as they are to be used as complements for the online collection of statements of support. Both Facebook and EU Login could provide a source to pre-fill the data fields, easing the process from a user perspective. In addition, both platforms offer the possibility to remove the CAPTCHA functionality.

Regarding the pre-filling of the data, both solutions provide divergent outcomes. EU Login is a relatively new platform, not widely spread across the EU. Besides, the data stored in the external accounts is reduced to the user's full name and his/her email, limiting its added value as users might

still have to enter the rest of the data manually. Moreover, due to the lack of a dedicated EU eIDAS node, severe limitations in its integration possibilities with OCS provided by third party prevent a wider use of this solution.

In contrast, Facebook is the most used social network, with a high degree of penetration in the EU. Although the data stored in Facebook accounts is not sufficient to cover the data requirements established in Annex III of the Regulation, implementing a connection with this social network could potentially expand the reach of the ECI tool, attracting a wider number of citizens and creating an additional campaigning platform for organisers. On the other hand, it should be noted that, according to Facebook's privacy policy, when users interact with third parties that uses Facebook's services (Log in, share, like, etc.), Facebook stores information about the usage of such services.

The table hereunder provides a comparison of these two similar solutions.

Evaluation Criteria	Solution 5	Solution 6	
Data Privacy	● ● ● ● ● ●	● ● ● ● ● ●	EU Login presents security features that make it a suitable solution for a potential integration with the OCS. On the contrary, regarding Facebook's privacy agreement, there is a concern regarding what specific information would Facebook have access to, and where this would be stored, regarding citizens and also organisers of any given initiative
Member States' responses	n/a	n/a	n/a
Ease of use	● ● ● ● ● ●	● ● ● ● ● ●	For both solutions, once the user authorises his/her data to be retrieved, the statement of support is automatically prefilled. There is a possibility to remove the CAPTCHA before submitting the statement of support.
Quantity of data	● ● ● ● ● ●	● ● ● ● ● ●	With EU Login external accounts, the user still need to enter most of the data manually. With Facebook, the quantity of data to be input by the user depends on each Member State's requirements.
Penetration	● ● ● ● ● ●	● ● ● ● ● ●	While EU Login is a fairly new service that is not currently used by a significant part of the EU population, Facebook has a penetration rate of 39.5% in Europe, meaning that over 307 million people have a Facebook account
Operational aspects	● ● ● ● ● ●	● ● ● ● ● ●	The operational aspects are similar for both solutions
Security	● ● ● ● ● ●	● ● ● ● ● ●	Both solutions presents similar score regarding security.
Integration	● ● ● ● ● ●	● ● ● ● ● ●	Both solution are easy to integrate, mature, portable and don't require a lot of effort or cost to be implemented.

Table 4: Comparison of solutions 5 and 6

1 INTRODUCTION

1.1 EUROPEAN CITIZENS' INITIATIVE

The European Citizens' Initiative (ECI) is one of the major innovations introduced by the Lisbon Treaty² and aims at involving citizens more closely in agenda-setting at EU level. The rules and procedures concerning the European citizens' initiative are set out in Regulation (EU) No 211/2011 (the ECI Regulation, hereinafter: the Regulation)³, which was adopted by the European Parliament and the Council in February 2011 and entered into effect on 1 April 2012.

As described in the Regulation, the whole ECI process comprises seven steps (see Figure 1), namely⁴:

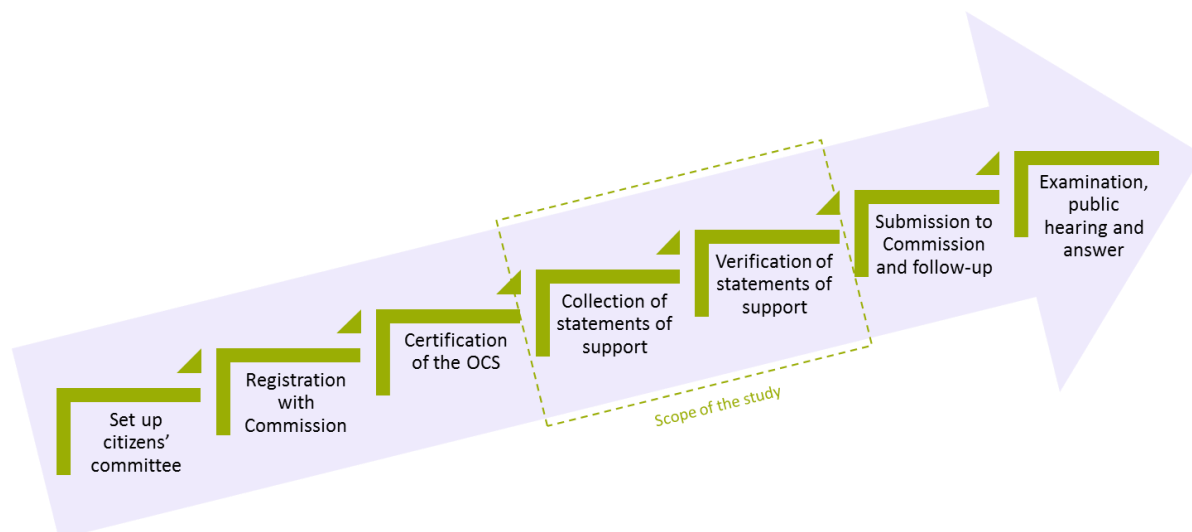


Figure 1: The ECI process

1. *Preparation and Setting up of the citizens' Committee.* In order to launch an ECI, organisers have to create a committee of at least seven citizens, who are residents of at least seven different Member States, of the age to be entitled to vote in the elections of the European Parliament (Article 3).
2. *Registration of the proposed initiative.* Before launching the collection of the statements of support from signatories, the organisers have to register the proposed initiative with the Commission, providing the information as required in Annex II of the Regulation (Article 4).
3. *Certification of the Online Collection System.* Organisers have to set up an Online Collection System that fully complies with the security and technical requirements set out in Article 6(4) of the Regulation on the citizens' initiative as well as with the Technical Specifications set out in Commission Implementing Regulation (EU) No 1179/2011. Once it is done, they should request the competent national authority where the data will be stored to certify the OCS. The authority has one month to verify if the specifications and requirements are satisfied. Once the system has been certified, the organisers receive a certificate.

² Article 11(4) of the Treaty on European Union and Article 24 of the Treaty on the Functioning of the European Union, which pertains to Union Citizenship

³ Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative (OJ L 65/1, 11.03.2011)

⁴ <http://ec.europa.eu/citizens-initiative/public/how-it-works>

4. *Collection of statements of support.* Once the initiative has been approved by the EC, the organisers can start collecting the statements of support, both on paper and online. In order to be successful, the initiative has to reach (1) the threshold of a total of one million valid statements of support, (2) the national threshold for each Member States in at least (3) a minimum of one quarter of the Member States needed. This phase of the process is the main focus of the study, with the verification of statements of support (Article 7).
5. *Verification of statements of support.* Once the collection phase has been completed and the one million threshold has been reached, organisers need to send the collected statements of support to the competent national authorities for verification and certification (Article 8).
6. *Submission of the initiative to the Commission.* After verification of the signatures, and given that the number of statements of support is still compliant with the Regulation, organisers can submit their initiative to the European Commission for evaluation. Within three months, the Commission is required to examine it and provide its legal and political conclusions on the initiative, including the action it intends to take (or the reasons for not taking action).
7. *Examination, Public Hearing and the Answer from European Commission.* Within three months, following Article 10, the organisers meet the Commission representatives to explain the details of the initiative they launched. They also have the opportunity, following Article 11, to present their initiative during a public hearing at the European Parliament. Finally, the European Commission answers by adopting a formal response detailing the actions it will propose and, if any, the reasons for doing or not doing so.

This study focuses on phases 4 & 5 of the ECI process, and only in the context of the online collection process.

1.2 OBJECTIVES AND SCOPE

In the five years of applying the Regulation, various ideas and studies have been expressed for improvement of the existing situation, in particular the report COM(2015) 145 on the application of the ECI Regulation⁵. Furthermore, building on the results of the study on ICT Impacts⁶, and more specifically recommendation N° 6: *Solutions to facilitate data entry and validation should be investigated*, this study aims at assessing the potential use of eID in the context of ECI – simplifying the online collection of statements of support and making it more efficient and user-friendly.

Recent progress in the field of eidentification could provide new technical possibilities in the process of the ECI. A substantial step towards a European-wide use of eID has been achieved since the eIDAS Regulation (Regulation (EU) No 910/2014 adopted on 23 July 2014). According to the Regulation, electronic identification and trust services for electronic transactions in the internal market must be recognised by all Member States. Accordingly, by 29 September 2018⁷, all Member States have to

⁵ European Commission, report from the European Commission to the European Parliament and the Council, Report on the application of Regulation (EU) No 211/2011 on the citizens' initiative, COM(2015) 145 final

⁶ European Commission (2015) Assessment of ICT impacts of the Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative

⁷ The eIDAS Regulation creates a European internal market for eTS - namely electronic signature, electronic seal, time stamp, electronic delivery service and website authentication - by ensuring that they will work across borders and have the same legal status as traditional paper based procedures. Only by providing certainty on the legal validity of all these services will businesses and citizens use the digital interactions as their natural way of interaction.

recognise any notified eID from any other Member State in all their eGovernment applications accepting their national eIDs.

The Online Collection System (OCS) is the part of the ECI process where the use of eID can have the greatest impact as it provides a secure and reliable stream of data that could ease the task of organisers and verifying authorities. It can improve the user experience for citizens by having a major impact on the simplification of the process of supporting an initiative. Besides, the use of eID in the ECI might generate various advantages, such as increased chances for validation or simplified (eliminated) verification process of statements of support. For this reason, the use of the eID to support an ECI should be taken into consideration and properly assessed.

Thus, the main objectives of the study are as follows:

1. Assess the legal, business and technical feasibility of using electronic identification to support an ECI (various scenarios and combinations of possible revisions of Annex III of the ECI Regulation and/or Commission Implementing Regulation (EU) No 1179/2011 are taken into account);
2. Assess several implementation options, in particular direct integration with national eID schemes and the use of the eIDAS framework;
3. Evaluate other options, such as electronic signature, EU Login, and integration with social networks;
4. Implement Proofs of Concept (POCs) demonstrating the technical feasibility of the solutions analysed in the study.

The analysis of each eID solution in the study covers three layers as depicted in Figure 2: the legal and business analysis (1) provide the basis for the elaboration of the solutions. In parallel, the technical analysis (2) is performed to assess the technical feasibility and later develop the technical specifications leading to the implementation of the PoCs (3).

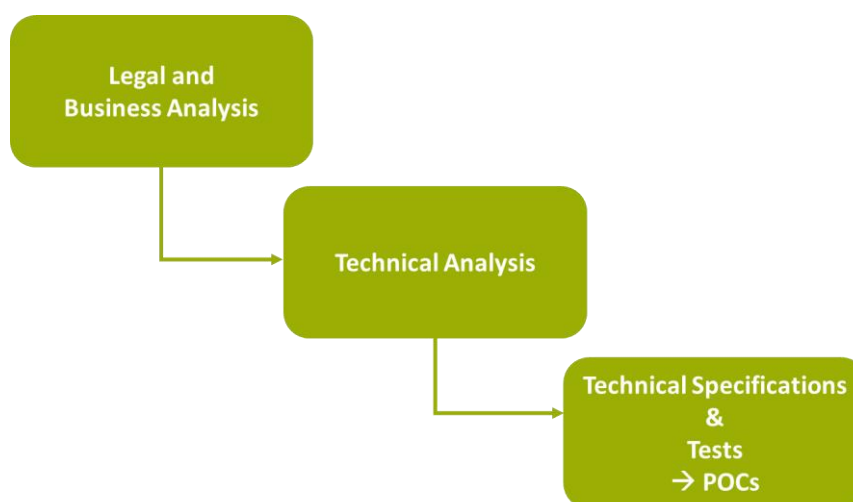


Figure 2: The three layers of the analysis

In order to assess the potential use of eID, the following aspects have also been analysed:

1. The challenges in the online collection process and systems for the ECI,
2. The benefits from the use of eID solutions.

As identified in the objectives, the study covers the analysis of six different solutions:

- Solution 1 – Electronically signed PDF: applying electronic signature on a statement of support in PDF format before uploading the document back into the OCS;
- Solution 2 – Integration of e-signature: using online electronic signature to sign a statement of support and perform the immediate validation of the signature;
- Solution 3 – Direct integration of eID: direct connection between the OCS and the national eIDs systems in order to validate the user’s identity online;
- Solution 4 –Integration with the eIDAS framework: indirect integration of eID via a connection through the eIDAS infrastructure in order to validate the user’s identity online;
- Solution 5 – Pre-filling with EU Login: prefilling user’s data in the statement of support by retrieving data from the user’s EU Login account;
- Solution 6 – Pre-filling with Facebook: prefilling user’s data in the statement of support by retrieving data from the user’s Facebook account.

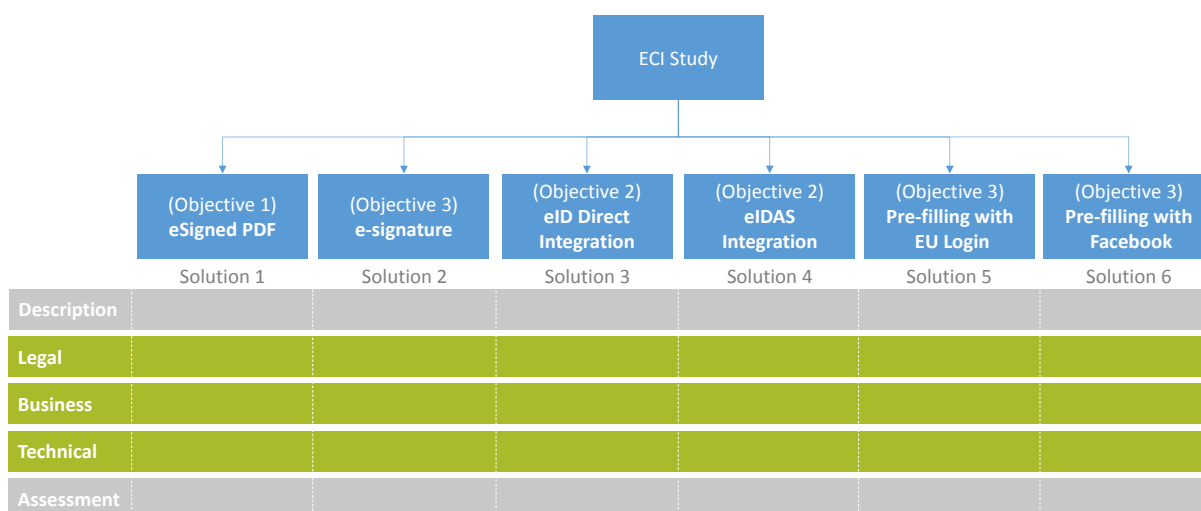


Figure 3: Breakdown of solution analysis

Correspondingly, each solution analysis breaks down as follows:

- First, a short description of the solution is provided.
- Then, the main findings of the legal, business and technical feasibility analysis are summarised.
- Finally, the final assessment of the solution, according to the evaluation criteria, is provided.
- In addition, as all solutions come two by two, a comparison of the pros and cons of both alternatives is made every two chapters.

1.3 STRUCTURE OF THE STUDY

The sequence of activities of the study is portrayed in Figure 4.

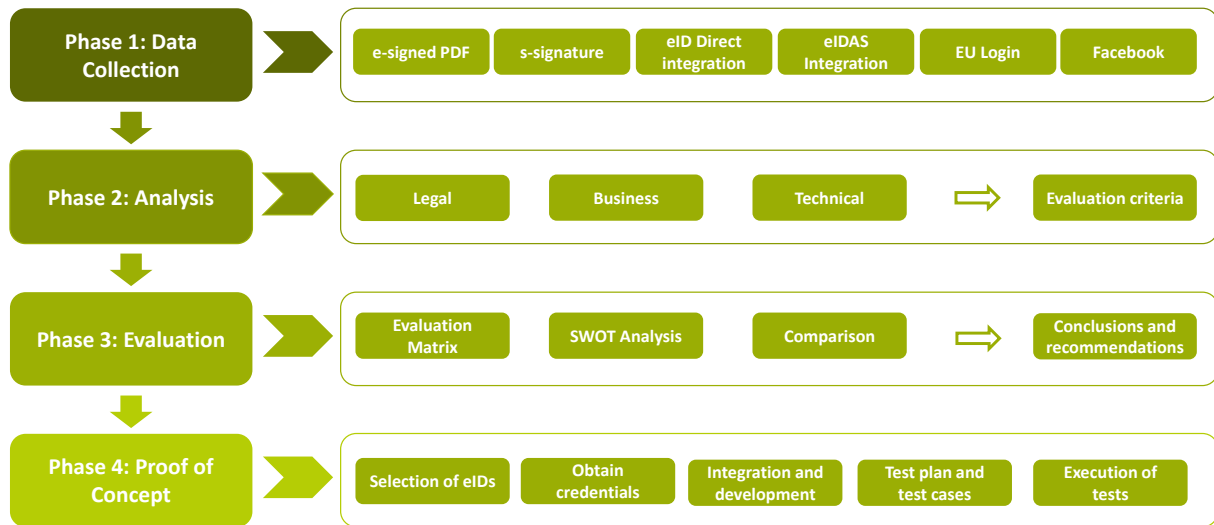


Figure 4: Sequence of the processes

Consequently, to achieve the general and specific objectives, everis structured the study as follows:

- Chapter 2 states everis approach to achieve the general and specific objectives following the three layers structure (Figure 4) and presents the methodology used throughout the study;
- Chapter 3 goes through three main components identified for this study: OCS, eID and eIDAS;
- Chapter 4 assesses solution 1: Electronically signed PDF document;
- Chapter 7 assesses solution 2: Integration of e-signature;
- Chapter 5 assesses solution 3: Direct integration of eID;
- Chapter 6 assesses solution 4: Integration with the eIDAS framework;
- Chapter 8 assesses solution 5: EU-Login as a pre-filling option;
- Chapter 9 assesses solution 6: Facebook as a pre-filling option;
- Chapter 10 provides the key conclusions drawn by everis, based on the key findings from the six solutions;
- Chapter 11 lists all the references used in this report; and
- Chapters 12 to 20 provide the support material and supplementary information as appendixes.

2 APPROACH AND METHODOLOGY

2.1 APPROACH

everis approach to achieve the objective is portrayed in Figure 5:

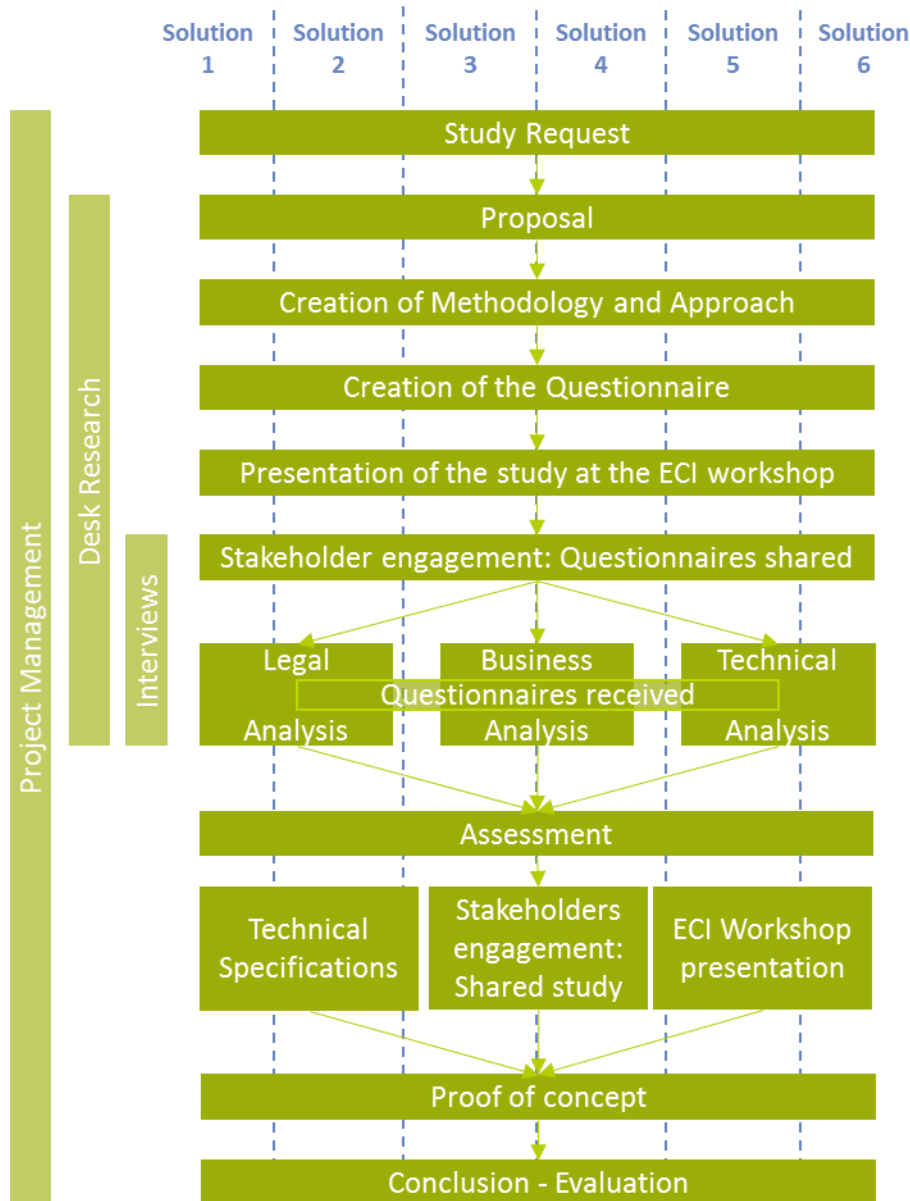


Figure 5: Approach

The identification of the methodology (see more detailed description in the following section) has been strongly influenced by the multifaceted analysis, covering legal, business and technical aspects of the selected solutions' implementation. Based on desk research, everis prepared the questionnaire that, covering the main questions for the solutions implementation, has served as a guiding checklist for the study and everis' consultations at the EU Member States' level.

The ECI Expert Group, established under Article 15 of the Regulation in conjunction with Article 6(3), has served as a platform for Member States and EC discussions on the ECI instrument, covering various aspects of the ECI and a number of areas for improvement. Selected questions from the questionnaire and the study itself have been presented during the meeting with the ECI Expert

Group on 22 November 2016. A consolidated version of the questionnaire was prepared following the comments made in the workshop and later shared with the ECI Expert Group. In parallel, given the highly technical content of several of the questions, the same questionnaire was shared with the eIDAS technical experts group to collect valuable information about the status of the technical solutions at Member States level. In the meantime, everis continued with desk research, interviews as well as legal, business and technical analysis.

The first phase consists in data collection, based on various desk research techniques, to identify the different eID solutions. In the second phase, the evaluation criteria are then guiding the analysis of the five identified eID solutions. Based on the analysis, the solutions are evaluated and conclusions and recommendations are drawn. Finally, based on those three phases, Proofs of Concept are developed and implemented.

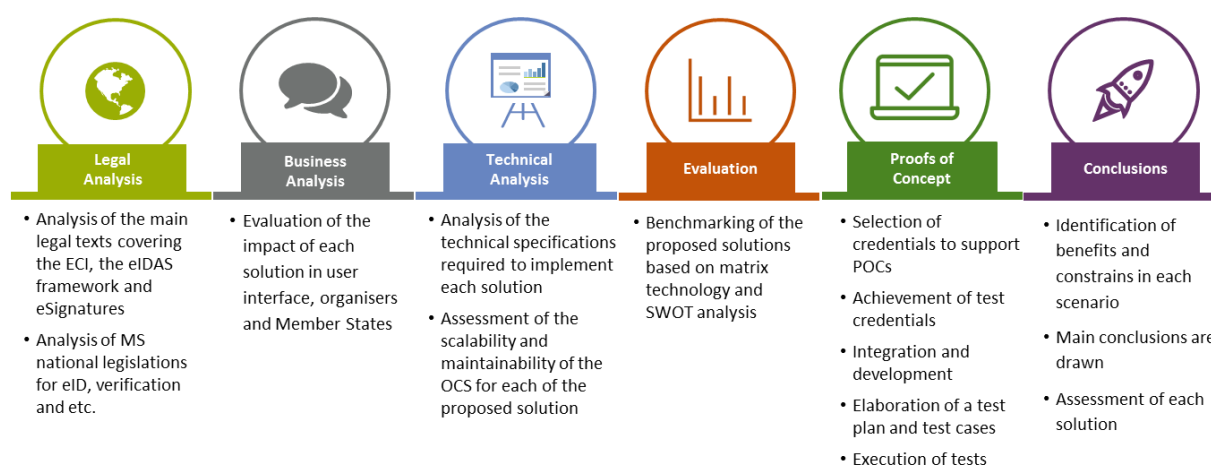


Figure 6: Components of the study

In order to assess the feasibility of using electronic identification to support an ECI, the study consists of six main elements. As defined previously, each solution is presented from legal, business and technical points of view, and its assessment is provided with an evaluation matrix criteria and a SWOT analysis. Additionally, this assessment is based on a comparative analysis with the AS-IS situation. Each solution assessment is followed by its technical prototype. Finally, the conclusions provide comparative analysis based on identified solutions' benefits, constraints and evaluation matrix.

Legal analysis:

The legal analysis includes, for every solution, the legal assessment and an insight to Member States' legislation relevant in each case. In addition, where relevant, the existing eID/e-signature laws and eIDAS regulation are analysed.

In respect to the Regulation, the particular emphasis is given to the online collection of statements of support (Articles 5 and 6), the verification and certification of the statements of support (Article 8) and the protection of personal data and liability for organisers of citizens' initiatives (Articles 12 and 13). Where applicable, the eIDAS Regulation analysis covers the scope of application, the mutual recognition of eIDs and the e-signature standards.

Methods applied: desk research, legal analysis, analytical method, micro analysis of a legal rule, case analysis, qualitative analysis, survey (questionnaire), and interviews.

Business analysis:

The business analysis sections provide the functional view of each solution in both phases of ECI: the collection and the verification of statements of support. It elaborates on the ease of use, the quantity of data (input), and the exploration of the penetration of the solution and existing awareness.

Methods applied: desk research, analytical method, document analysis, qualitative analysis, use case, workshop, interviews and survey (questionnaire).

Technical analysis:

The technical analysis is two-fold. First, the quality of the eIDs and/or e-signatures are analysed in regards to the data available in them and its compatibility with the ECI requirements. Second, each solution is explored based on seven selected evaluation criteria, namely: ease of integration, scalability, maintainability, performance, security (data storage, fraud prevention, data transmission and session management), and costs/efforts.

As each solution might have different implementation alternatives, some involving different architectures, others implying different scopes or procedures, all these alternatives are identified and analysed along the study.

Methods applied: desk research, document analysis, interviews and survey (questionnaire), qualitative analysis, analytical method

Evaluation:

Each solution is assessed based on two different techniques: evaluation matrix and SWOT analysis.

Methods applied: Evaluation matrix criteria, SWOT, analytical method, comparative analysis

Proofs of Concept (Disclaimer: not published with the study report)/Technical integration:

In order to validate the analysis, Proofs of Concept are developed. For the selected solutions, the required software is integrated into the OCS and tested with a set of national eIDs. The purpose is to detect any problem not foreseen in the analysis. As a consequence, the quality of the documentation and developed code may not meet “production ripe” standards

Evaluation/Final conclusions:

Two by two, the solutions are evaluated and compared, covering the main aspects of the SWOT analysis and the evaluation matrix. The final conclusions and recommendations are drawn for the possible future eID integration into the ECI.

Methods applied: comparative analysis, analytical method, evaluation matrix

2.2 METHODS AND TECHNIQUES

To carry out this study, gather information and conduct a qualitative analysis of the different eID solutions to support an ECI, the following methods are used:

- **Interviews:** Qualitative and in-depth interviews were conducted with key stakeholders to collect additional data and information, also as a follow-up of questionnaires.
- **Workshop(s):** The main objective of the workshops is to facilitate knowledge, information and insights sharing. The ECI Expert Group Meeting⁸ offered the possibility to meet most of the representatives of the Member States and to start the discussion on the implementation of eID solutions for the ECI. The following ECI Expert Group Meeting might facilitate the forum for the discussion of the results of this study.
- **Questionnaire:** A pre-filled questionnaire, summarising the data collected and indicating missing information, has been shared with Member States' representatives. This questionnaire brings an important contribution to the study as the answers received from the Member States are used to develop and complete the analysis.
- **Document analysis:** The identification of relevant sources (literature review: previous studies, reports, legislations, general papers, articles etc.) regarding the ECI and eID is the main output of desk research. During this phase, documents, including legal, were analysed to gather data and information related to the study.
- **Use case:** The use cases are used to illustrate the user requirements by describing sequences of interactions between the user and the ECI platform. It captures the visible functions in parallel with the user's actions relevant to his/her goal. To ease the understanding of the impact of each proposed solution on the user interface, use cases systematically describe in details the steps and procedures the user will follow.
- **Benchmarking:** The evaluation of each eID solution is structured along three main domains: legal, business and technical. In order to evaluate the success of each solution against every domain, a set of evaluation criteria is developed. Each criterion addresses a specific element that needs to be considered during the analysis. The benchmarking analyses the various proposed solutions, as well as the already existing one, based on two methods: **Matrix technology** and **SWOT analysis**.

Evaluation Matrix

To develop the Evaluation Matrix for each eID solution, the following steps are followed:

1. Based on the three domains, a list of evaluation criteria, determining the success of the solution, is constructed.
2. A score is assigned to every evaluation criterion. A weakness is represented by a low score (1 or 2) while advantages are represented by a high score (4 or 5). A TO BE situation similar to the AS IS situation will usually get a median score of 3.

Domain	Criteria	Score
	Criteria	Score
	Criteria	Score
	Criteria	Score
	Criteria	Score
	Criteria	Score
Total Score		

Figure 7: Evaluation Matrix

⁸ ECI Expert Group Meeting – 22 November 2016

3. By summing the scores of all the criteria, the total resulting score of the solution is obtained.

The score of each evaluation criterion can vary from 1 to 5. It is calculated based on a comparison between the ideal situation defined for each criteria and the current situation. The closer the AS-IS situation is from the ideal one, the better the score.

SWOT analysis

The SWOT analysis focuses on the strengths, weaknesses, opportunities and threats of each eID solution. It aims at identifying the internal and external criteria influencing, in a helpful or harmful way, the solution. The internal criteria represent the strengths and weaknesses internal to the eID solution while the external criteria represent the opportunities and threats coming from the external environment.

When conducting a SWOT analysis, the aim is to list, within the table, both the internal and external factors. The final objective being to identify the impact of the different evaluation criteria on each eID solution.

	Helpful	Harmful
Internal Origin	Strengths	Weaknesses
External Origin	Opportunities	Threats

Figure 8: SWOT analysis

- **Technical integration:** The implementation of the Proofs of Concept, demonstrating the feasibility of the proposed solutions, is divided into five main steps:
 1. **Selection of eIDs to support the prototype:** Based on the available and usable eIDs, Member States are invited to participate in the PoCs. From the volunteering Member States, a selection is made in order to achieve the maximum representation of the EU population, while not increasing the required efforts.
 2. **Achievement of test credentials:** The Member States participating in the PoCs are requested to provide eIDs valid in their preproduction environment. These eIDs are necessary for performing tests on the integration of their national eIDs into the OCS, according to the solution. These eIDs are similar to ones issued to the citizens, the only difference being that they are only valid in their preproduction environment and not in production.
 3. **Integration and development:** The solution, as described conceptually in this study, is detailed with a functional and technical design before developing and integrating the corresponding software. The designs will comply with the “PoC quality requirements”: including all essential contents for development and integration, but not oriented towards the maintenance of the solution.
 4. **Elaboration of a test plan and test cases:** The test plan describes the procedure and responsibilities for testing, mostly oriented towards testing tasks and responsibilities for different organisations. Testing tools may be recommended, as far as their use is considered very beneficial for this project. The test cases enumerate the alternatives scenarios to be tested, the conditions under which they should be performed and the expected results. Test cases can be positive or negative. Negative tests include cases in which the input should be rejected. All test cases determine the functioning of the

modules integrated into the system under normal circumstances: they exclude performance tests, penetration tests, etc.

5. **Execution of tests:** For each test case, the circumstances under which the test should be performed are produced and the test is carried out. An internal test status report is maintained, indicating the results of the tests for each test case. If the expected results are not produced, a description of the results is included, containing information allowing the developer to reproduce the error. After finalizing the tests, the last version of this report is delivered to the European Commission.

The above-mentioned criteria selected for both the Matrix Technology and the SWOT analysis methods, as well as their respective domains, are listed as follows:

Domain	Criteria	Description
Legal	ECI Regulation	Conformity with the Regulation is assessed taking into account possible modifications to fit the implementation of the solution
	eIDAS Regulation	Conformity with the rules and standards of the eIDAS regulation is assessed
	Member States' responses	The responses from the Member States are analysed regarding each solution
Business	Ease of use	Is it easier to support an ECI thanks to the solution?
	Quantity of data (input)	How much data needs to be filled in by the user?
	Penetration level/awareness	Does the solution have a positive impact on the awareness level of the ECI tool? Does it help to improve the penetration level of ECI?
	Scalability	Will the solution present scalability issues?
Technical	Maintainability	Is the maintainability of the solution demanding or not significant?
	Performance and usage of resources	How big is the impact of the solution on the performance of the ECI website?
	Security on Data storage	What is the level of security regarding the data storage of the solution? Are the data stored according to the EC requirements?
	Fraud prevention	What is the level of security regarding the fraud prevention of the solution? To which extend is the solution "protected" against fake/multiple accounts/users/signatories?
	Security on data transmission	Are the integrity and confidentiality of the data guaranteed during their transmission?
	Session Management	If the statements of support are transmitted in more than one session, how is the relation between the sessions secured?
	Ease of integration	How complex is the integration: is an API available, what is the complexity of the integration software, etc?
	Maturity	For how long has the solution been working, is used by many people and portals?
	Portability	Is the solution portable to different operating systems and Internet browsers?
	Costs/efforts	How much costs and effort does the implementation of the solution require?

Table 5: Description of the evaluation criteria

3 OVERVIEW OF THE MAIN COMPONENTS

3.1 THE ONLINE COLLECTION SYSTEM (OCS)

The ECI Regulation as well as the Implementing Regulation 1179/2011 set out the conditions, legal requirements and technical specifications for the Online Collection System in the context of the ECI. The Online Collection System is intrinsically linked to the third step of the ECI process: collection of signatures. Indeed, in order to collect the statements of support online, it is required that the organisers have:

- A server to store the data of the signatories
- A software allowing the online collection of statements of support

Once registration is confirmed, the organisers have 12 months to collect the one million signatures, both on paper and online, through an OCS certified by the Member State in which it is located.

As organisers were facing substantial difficulties to find appropriate Online Collection Systems and hosting providers, the Commission provided servers of its own in Luxembourg. The EC also developed, maintained and improved its own open-source Online Collection System, which was temporarily offered free of charge to the organisers. Later, the European Commission committed itself to continue its hosting practice for free as long as needed⁹.

3.1.1 Challenges and opportunities

Studies, reports and recommendations from the ECI expert group acknowledge the main issues that the ECI is currently facing. The current framework provides an operational ECI, although there is room for further improvement. Figure 9 provides an overview of the main challenges and opportunities to improve the online collection of signatures process.

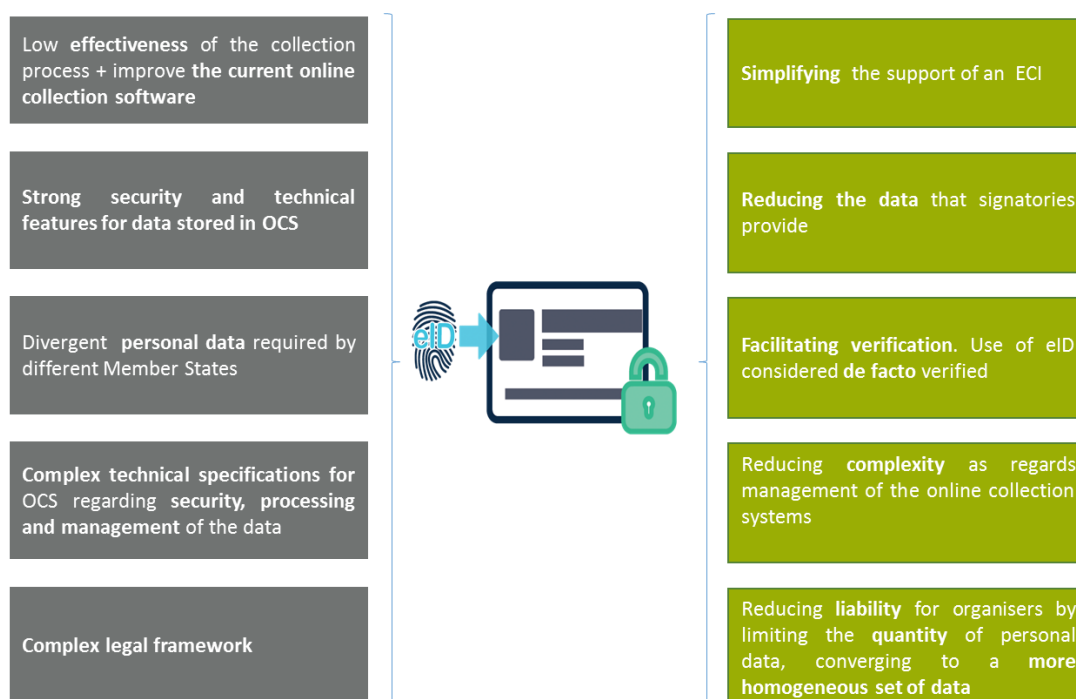


Figure 9: Challenges and opportunities

⁹ <http://ec.europa.eu/citizens-initiative/public/hosting>

Within the scope of this study, some key challenges can be highlighted:

- Need to increase the effectiveness of the collection process and to improve the current Online Collection System.
- Storage of personal data through the Online Collection Systems, thus requiring to meet high security and technical standards.
- Important divergences, in regards to the personal data required by the different Member States, make the support of an initiative and the verification of the identity of the signatories tedious and time consuming.
- Complexity of the current legal framework, where Member States are responsible for the implementation of many requirements.
- Complex technical specifications for the Online Collection Systems related to the security, processing and management of the data during the ECI lifecycle.

In light of those challenges, the following specific objectives and evaluation criteria were set:

- Legal compliance with regards to the applicable legislation (ECI Regulation and eIDAS Regulation when relevant).
Criteria: **ECI Regulation** and **eIDAS Regulation**
- Simplified, more efficient and more user-friendly process for the signatories for supporting the ECI online.
Criteria: **ease of use** and **penetration**
- Reduction and/or elimination of the data that needs to be provided by signatories.
Criterion: **quantity of data**
- Facilitation (elimination) of the verification process of statements of support, as using the eID in the ECI online could be considered as de facto verified by Member States.
Criterion: **Member States' responses**
- Liability reduction for the organisers by limiting the quantity and sensitivity of the collected personal data.
Criterion: **security**
- Technical feasibility.
Criteria: **operational aspects** and **integration**

Furthermore, the following opportunities can be seized in case the eID solution is implemented:

- Simplifying the process of supporting an ECI online and making it more user-friendly for the signatories.
- Reducing or eliminating some data that the signatories need to provide.
- Facilitating the verification process of statements of support by the Member States.
- The citizens using eID options to access the signing process could be considered as being de facto verified.
- Reducing complexity for organisers in regards to setting up and managing the Online Collection Systems.

- Reducing the liability for the organisers by limiting the quantity of personal data, thus converging to a more homogeneous set of data required across all Member States.

3.2 EID CURRENT STATE OVERVIEW

3.2.1 Introduction

Regarding the possible implementation of the national eID into the current ECI legislative framework, the research carried out so far shows that many Member States have already deployed functional eID schemes. However, the system chosen might vary to a great extent. Investments were made in different technologies at different times, and consequently, national governments chose the most suitable national eID scheme among the different alternatives. The current situation shows that there are several parallel eID tools living together at the same time, and that the data stored in those credentials is different.

Furthermore, it is important to mention that although some countries have chosen a publicly-managed system (e.g., Belgium, Estonia, Germany, Spain, and Portugal), most countries tend to develop a system relying on private entities that, under public authorisation and supervision, issue valid eIDs that can be used to access both private and public services.

In this context, leveraging electronic identification to support an ECI aims to achieve two main goals:

1. Citizens would be able to reduce the quantity of sensitive personal data that they have to enter online, and in the best case, they won't even have to enter anything at all;
2. The statements of support could be automatically verified on the spot and validated by the Member States, only requiring to check for duplicates. This innovation increases the ratio of valid statements of support and enhances the overall efficiency of the system.

The integration of national electronic identification means of the Member States into the online collection systems is also to be assessed, with the possibility to make it consistent with the eIDAS regulation framework.

General concepts about electronic identification and electronic signatures are explained in the following sections in order to provide the background information needed for apprehending the analysis that have been carried out.

3.2.2 Electronic identification

The evolution of Information Technology (IT) derived into a wide array of services and tasks that users can make use of. Besides, certain elements require specific permissions to be accessed. This requirement created the need to differentiate the users via electronic identification (eID), especially when dealing with sensitive data and private communications.

Three factors for authentication of a user can be distinguished, from the most complex to process to the least:

- The characteristic of the person, or biometrics: fingerprints, photos, etc.
- The objects or tools that users have in their possession: mobile phone, smartcard, code card, security token, etc.
- The information only known by the users: especially passwords

It is considered that authentication systems based on only one of these three factors are not secure enough; at least two factors are required for optimal security.

The purpose of the remaining of this section is to define and explain the key concepts with regards to eID and e Signature, which will be discussed in the assessment of the different solutions.

Username / password schemes

The oldest eID authentication method is based on the combination of a username and a password: the user introduces his username and password, and the system looks up the user and compares the introduced password with the stored password. As this method is only based on the third factor (information only known by users), it is not considered secure enough in this context.

Several variations have been invented on this scheme, including one-time passwords (OTP) generated by a special user-held device¹⁰ or sent by SMS. These variations aim to reinforce the quality of authentication by including additional factors.

PKI and certificates

A somewhat different approach on eID is offered by PKI (Public Key Infrastructure): this technique is based on information under control of the user, allowing the verification of its private key without disclosing it.

PKI is based on a collection of algorithms and two keys: a private and a public one (key-pair). The public key is designed to be available to any interested person while the private one is only available to its owner. These keys are created in a way that what is encrypted with one key can only be decrypted with the other one. The main difference with username / password schemes is that while the private key is similar to a password, it does not have to be stored in a central database and sent across the network at each authentication.

The algorithms are designed to process any data with either key. If the process is performed with one key and the original data, these data results are encrypted. If it is performed with the other key and the encrypted data, these data results are decrypted.

Therefore, a message encrypted with the public key can only be decrypted with the private key, ensuring the confidentiality of the exchanged data. Similarly, a message encrypted with the private key can only be decrypted with the public key, ensuring both the integrity of the data and the fact that the owner of the private key is the author of these data.

PKI management: Certificates & Certifications Authorities

In order to make sure that a key-pair belongs to a certain person, this key-pair is certified by a Certification Authority (CA) to belong to the subscriber. The certificate¹¹ includes:

- The personal data:
 - The subscriber's common name (CN)
 - The organisation (O)
 - The organisational unit (OU)
 - The country (C)

These four data items form the citizen's Distinguished Name (DN), which must be unique within the set of certificates issued by a CA.

¹⁰ <https://www.rsa.com/en-us/products/identity-and-access-management/authentication-and-identity-assurance>

¹¹ RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

- The subscriber's public key
- A serial number: The serial number of the certificate must also be unique within the collection of certificates issued by one CA.
- The name and optionally the identifier of the issuing CA
- The validity: it includes two timestamps: *notBefore* and *notAfter*, limiting the validity period
- The extensions: there are two main relevant extensions, developed in the next section: the key usage and the object ID (OID).
- The Certification Authority signature

The certification authority can be held responsible for the data being accurate and belonging to the identified person. This responsibility is usually difficult to enforce for an international usage, inter alia due to language problems. However, if the certificate is used through the eIDAS framework, the national eIDAS authority can enforce this responsibility basing itself on the eIDAS Regulation.

The natural life cycle of a certificate is given by its expiration date (*notAfter* of the validity). However, if the certificate has been stolen or if the subscriber suspects that the private key has been compromised, it can be revoked before the expiration date in order to prevent any impersonation of the certificate's owner. Revocations are published by the CA (or by any other authorised organisation) in a Certificate Revocation List (CRL). The scope of the CRL is indicated in this list, which could be, for example, all certificates of the CA or all certificates signed with one of the CA's certificates. Another difference between CRLs is its completeness: CRLs can be complete or partial (delta).

Key usage

As described in the previous section, the algorithms are designed to process any data with either key. As the user should be aware what operation is being performed, the key-usage attribute is included in the certificate, limiting these operations. The key usage limits the operations which can be performed with the key-pair of the certificate, in order to allow the subscriber to know which operation is being performed on his behalf.

Values for key usage, which are relevant in the scope of this document are:

- digitalSignature
- contentCommitment (formerly nonRepudiation)
- dataEncipherment
- id-kp-clientAuth

It is common practice to allow only the creation of digital signatures with one certificate, and perform other functions with another one. In cases two certificates are issued to the same person, one for the signature and the other for the authentication and/or the encryption, only the key-usage, keypairs and the serial number are different. All other data of the certificates are the same. For instance, expiration date and personal data are identical in both certificates.

Object ID (OID)

Certificates are issued under certain conditions, for a specific part of the population and for a particular purpose: this is summarised in the certification policy. One CA may issue certificates under different policies, but each certificate is issued under one policy only. This policy is indicated in the Object ID (OID).

Some relevant issues which can be understood from the certification policy are:

- Is the certificate stored in a cryptographic device?
- Is the subscriber a natural person, acting on behalf of himself?
- Is the subscriber a natural person, acting on behalf of another person?
- Is the subscriber a legal person?

The OID's format is a string of numbers separated by dots. The first part of this string is standardised, up to the number which identifies the CA. Each CA may personalise the rest of the string. In order to know the relevant elements mentioned above, the written CA's certification policy must be interpreted by human beings.

Authentication with certificates

The most common authentication method with certificates uses either Secure Sockets Layer (SSL) or Transport Layer Security (TLS) technologies. TLS is the updated, more secure version of SSL, but all these methods are commonly referred to as SSL. SSL Certificates, sometimes called digital certificates, are used to establish a secure encrypted connection between a browser (user's computer) and a server (website). The SSL connection protects sensitive data exchanged during each visit (session). This is the minimum requirement to ensure server authentication. Additionally, a user authentication can be configured, which implies that the browser will request the user to select an available certificate. Together with the request from the server to the browser, a random number, a "seed", is included. The browser encrypts the seed with the private key of the user. This encrypted seed, together with the user's certificate, is included in the response to the server, which decrypts the encrypted seed with the user's public key and verifies that the result is the same as the sent seed. Afterwards, it extracts the user's identity from the certificate.

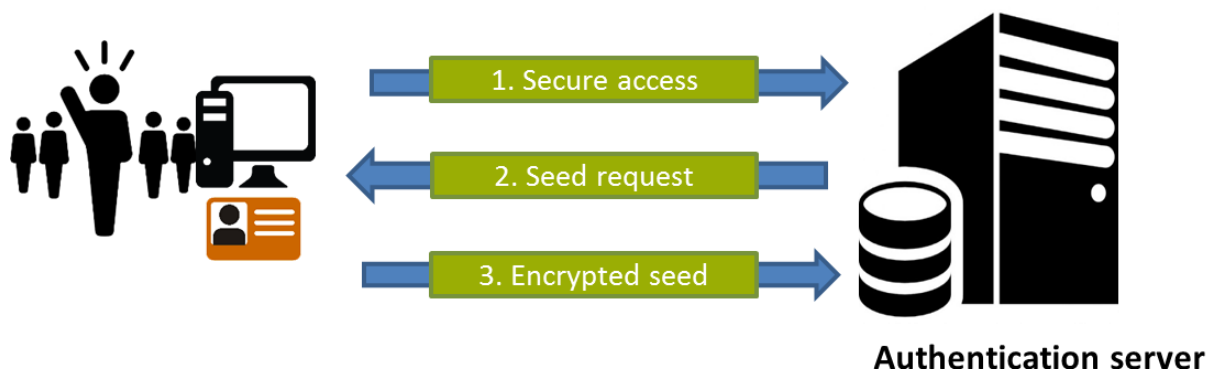


Figure 10: Process of authentication with certificates

Quality of authentication

Within the wide variety of eIDs, there is also a wide variety of authentication qualities: a simple username / password method is less reliable than a certificate stored on a cryptographic device. Even within the username / password method, different quality requirements on the password will lead to different qualities of authentication.

In 2008, the STORK project studied the authentication quality and then proposed and implemented an internal standard, called QAA (Quality of Authentication Assurance), taking into account the basic factors for quality of authentication. The first four factors defined by STORK¹² apply to the registering and issuing procedure, the next three criteria apply to the eID itself and its usage.

¹² In its deliverable 2.3 Quality Authenticator Scheme

In 2010, the OASIS workgroup published its own version¹³ of a scheme for simplifying the quality of the authentication process, similar to the STORK standard, naming the quality of authentication “Level of Assurance” (LoA). This version was adopted by the ISO and the NIST.

The eIDAS regulation based its definition for the quality of authentication on the STORK quality definitions, improved it with the OASIS contributions, and kept the name “Level of Assurance”. Whereas STORK and OASIS numbered these levels from 1 to 4, eIDAS uses only three levels: low, substantial and high, more or less corresponding with levels 2 to 4 of the previous standards. Once the user is authenticated, these LoAs are sent to the portal which issued the authentication request.

Whereas the previous paragraphs refer to the quality as a result of the authentication process, the eIDs themselves may also have a quality indicator: qualified certificates meet the criteria specified in Annex I of the eIDAS Regulation and are issued by a qualified and trusted service provider, i.e. a service provider which is granted to be qualified by the supervisory body, and which offers qualified services. Non-qualified certificates, which don’t meet these criteria, are attributed a lower quality level. While certificates can be qualified according to the requirements of the eIDAS regulation, other eIDs cannot. However, these eIDs can be of substantial level of assurance if they meet the requirements for this level.

3.2.3 Electronic signatures

Considering the algorithms, an e-signature can be produced using a private key on any original dataset. In practice, the whole dataset is not encrypted with the private key as it would be a time-consuming process: several minutes for a normal 100k file. Instead, a hashing function is applied to the dataset, summarising it into 160 or 512 bits¹⁴. The hashing mechanism makes sure that it is virtually impossible to generate a file which results in the same hash value.

This hash value is encrypted with a private key; the encrypted value is then stored together with the certificate in the e-signature. This way, the e-signature provides a unique link to the signed data, with the encrypted value of the hash, while the signatory is identified with the certificate.

Standardised signature formats

The first standard signature format was PKCS#7; in essence it included the encrypted hash and the certificate as described in previous paragraph. More recent signature standards now fully integrate the signature with the signed data in a common structure. Three industry standard formats¹⁵ exist:

- Signed PDF documents: PAdES, or PDF Advanced Electronic Signature
- Signed XML data: XAdES or XML Advanced Electronic Signature
- Signed any other data: CAdES or CMS Advanced Electronic Signature; CMS is Cryptographic Message Syntax

These formats have been adopted by the EC by means of the Commission Implementing Decision (EU) 2015/1506¹⁶.

¹³ <https://www.oasis-open.org/committees/download.php/44751/285-17Attach1.pdf>

¹⁴ SHA1 used 128 to 160 bits. The more modern SHA2 normally uses 256 or 512 bits.

¹⁵ ISO standard 32000-1: <https://www.iso.org/standard/51502.html> and ETSI standard TS 102 778:

http://www.etsi.org/deliver/etsi_ts/5C102700_102799%5C10277801%5C01.01.01_60%5Cts_10277801v010101p.pdf

¹⁶ <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1506&from=EN>

Typical signature creation environments and methods

Most PDF readers allow the creation of PAdES signatures, allowing the user to select the certificate, which is to be used for creating the e-signature. After the signature is created in the document, it needs to be saved as a signed document. This process is executed offline, on the user's PC or mobile device.

The most widely used environment for the creation of XAdES signatures is a web-page, e.g. in a banking application for money transfer. The data to be signed is sent to the browser, usually in a hidden HTML field in a form, reserving another field for providing the signed data as the response. With this data, an active element in the user's PC is invoked for the signature creation. Until recently, an applet was used for this purpose. However, since Google announced¹⁷ that it would stop supporting applets in Google Chrome, such applets have been substituted by other solutions.

Those solutions retrieve the XML data to be signed, display them to the user, request the user to select a certificate with which to produce a signature, and produce a XAdES signature. This signature is returned to the browser in the field reserved for the signature. The browser finally sends the data of the HTML form, including the XAdES signature, to the server.

CAAdES signatures can be produced online as well as offline, with any data and without any requirements on the format of these data. Consequently, there is no typical environment for creation of CAAdES signatures, as this is the least used format for signatures. Regarding offline documents, PAdES is the most used format, while for online data, XAdES is the most used one.

The European Commission, through the Connecting Europe Facility's eSignature Building Block, provides the DSS open-source library, which supports the creation and validation of electronic signatures (as well as electronic seals) in line with the eIDAS Regulation and related standards, including XAdES, PAdES and CAAdES¹⁸.

Quality of signatures

Although all industry standards for e-signatures are based on certificates, other methods can produce e-signatures. Nonetheless, their quality is lower, as no other method than PKI currently allows proof that the user has agreed with the signed data, without including his secret information: password or private key as the proof of his identity.

In that sense, the eIDAS regulation establishes in Article 26 that an advanced signature is a signature which meets the following requirements:

- It is uniquely linked to the signatory.
- It is capable of identifying the signatory.
- It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control.
- It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

In practice, the only known method for creating such signatures is using PKI certificates. Previously mentioned methods, such as username / password schemes, do not comply with the eIDAS

¹⁷ <https://blog.chromium.org/2013/09/saying-goodbye-to-our-old-friend-npapi.html>

¹⁸ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature>

requirements for advanced e-signatures. The last requirement is especially hard to fulfil without using the PKI technology.

The eIDAS Regulation additionally establishes the level of a 'qualified electronic signature'. Qualified electronic signatures are advanced electronic signatures which additionally are:

- Created by a so-called 'qualified electronic signature creation device'. Qualified electronic signature creation devices are certified as such by Member States according to a set of defined standards.
- Based on a so-called 'qualified certificate'. Qualified certificates can only be issued by so-called qualified trust service providers, which are made public by Member States through Trusted Lists.

The eIDAS Regulation stipulates that qualified electronic signatures shall be recognised as equivalent to handwritten signatures across the European Union.

3.2.4 Overview of national eID schemes

This study summarises information about national eID systems in each Member State based on the input received from the Member States.

Each Member State's eID solutions are based on Levels of Assurance (LoA). They describe the authorities' degree of trust that the user has presented an identifier, a credential in this context, which refers to his/her identity. In this case, the assurance is defined as (1) the degree of confidence in the registration and issuing process used to verify the identity of the individual to whom the credential was issued and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. In the eIDAS message format¹⁹, as part of the technical specifications, the LoA is defined as: Low, Substantial or High. The details of the main eID solution in each Member State can be found in Appendix A.

¹⁹ eIDAS SAML message format available at https://joinup.ec.europa.eu/sites/default/files/eidas_message_format_v1.0.pdf

3.2.5 Overview of the eID available data

Legend	
x	Data present on the eID
	Data not present on the eID
	Missing information

	Name		Fathers'		Name		Residence		Date		Place		Nationality		Personal	
	ECI Personal data requirements	eID Data	ECI Personal data requirements	eID Data	ECI Personal data requirements	eID Data	ECI Personal data requirements	eID Data	ECI Personal data requirements	eID Data	ECI Personal data requirements	eID Data	ECI Personal data requirements	eID Data	ECI Personal data requirements	eID Data
Austria	x	x					with full address details		x	x	x		x		x	x
Belgium	x	x					x	x	x	x	x	x	x	x		x
Bulgaria	x		x										x		x	
Croatia	x						with full address details						x		x	
Cyprus	x												x		x	
Czech Republic	x	x						x		x			x	x	x	x
Denmark	x						x		x		x		x			
Estonia	x	x					x		x	x	x					x
Finland	x	x					Only the country		x	x		x	x	x		x
France	x						with full address details		x		x		x		x	
Germany	x	x				(x)	x		x	x	x	x	x	x		
Greece	x	x	x	x	x				x	x					x	x
Hungary	x	x		x		x		x		x		x	x	x	x	x
Ireland	x						x		x				x			
Italy	x	x					with full address details	x	x	x	x	x	x	x	with issuing authority	x
Latvia	x	x			x				x	x	x		x	x	x	x
Lithuania	x	x								x			x	x	x	x
Luxembourg	x	x					with full address details	x	x	x	x	x	x	x		x
Malta	x	x							x	x		x	x	x	x	x
Netherlands	x	x			x		x	x	x	x	x	x	x	x		x
Poland	x						with full address details						x		x	
Portugal	x	x		x				x	x	x			x	x	x	x
Romania	x						with full address details		x				x		x	
Slovakia	x	x			x		x	x	x	x	x	x	x	x		x
Slovenia	x								x		x		x		x	
Spain	x	x		x				x	x	x		x	x	x	x	x
Sweden	x	x								x			x	x	x	x
UK	x						x		x				x			

Table 6: Overview of the eID available data

3.3 EIDAS CURRENT STATE OVERVIEW

The Regulation (EU) 910/2014²⁰ (eIDAS Regulation) establishes the Electronic Identification Authentication Services, the legal framework for accepting eIDs and trust services across the EU. It was adopted in July 2014 and entered into on 17 September 2014.

The 52 Articles of the new Regulation cover different aspects of electronic transactions²¹:

- Electronic identification
- Trust services, comprising:
 - Electronic signatures, seals and time stamps
 - Electronic registered delivery services
 - Certificates for website authentication
- Electronic documents

Although eIDAS has already entered into force, the Regulation foresees different legal deadlines in order to give all Member States time to prepare and adapt their regulations and infrastructures.

In regards to authentication (verification of the identity of a signatory), the established deadline is set on 28 September 2018. By that time, all Member States should accept all foreign eIDAS credentials in all their eGovernment applications that require access to national credentials. Some countries are quite advanced and are already able to notify and receive information, but until all Member States achieve integration into the framework, eIDAS full potential will not be maximised.

On the other hand, e-signature is an already existing technology that has been present in Member States since the Electronic Signature Directive of 1999. Regarding this specific aspect of the Regulation, according to some Member State representatives interviewed, the interoperability framework can be considered as totally functional.

Member States are currently working to adapt to the eIDAS regulation by performing the following actions:

- (Pre-)notifying their national eIDs to be used within the eIDAS network according to the agreed procedure
- Establishing their national eIDAS node, integrated with their national eID infrastructure
- Connecting existing eGovernment services to their eIDAS node

A few Member States already have their eIDAS node available in production, integrated with their eID infrastructure. As a matter of fact, recently, countries like Austria, Germany and the Netherlands have managed to connect their identification and authentication systems via their (technically compliant) eIDAS nodes in production²². Until all Member States' eIDs have been formally notified, those nodes cannot be considered as being fully operational. It can however be expected that some additional nodes will be available for use within the coming month.

²⁰ http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

²¹ Bender, Jens (2015) eIDAS Regulation: eID-Opportunities and Risks. Fraunhofer-Gesellschaft, session V: Standardisierung. p.156-166; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Bender.pdf?__blob=publicationFile

²² <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Key+Milestone+Reached%21+First+Cross+Border+Connections+Between+%28technically++compliant%29+eIDAS+Nodes+in+Production>

3.3.1 Overview of the eIDAS dataset and ECI personal data requirements

Legend	
x	Present/Required
	Not required/not present
	Present in the eIDAS Optional Data Set

	Name		Fathers' name		Name at birth		Residence		Date of birth		Place of birth		Nationality		Personal Identification Number	
	ECI Personal data requirements	eIDAS	ECI Personal data requirements	eIDAS	ECI Personal data requirements	eIDAS	ECI Personal data requirements	eIDAS	ECI Personal data requirements	eIDAS	ECI Personal data requirements	eIDAS	ECI Personal data requirements	eIDAS	ECI Personal data requirements	eIDAS
Austria	x	x				x	with full address details	x	x	x			x		x	x
Belgium	x	x				x	x	x	x	x			x			x
Bulgaria	x	x	x			x		x		x			x		x	x
Croatia	x	x				x	with full address details	x		x			x		x	x
Cyprus	x	x				x		x		x			x		x	x
Czech Republic	x	x				x		x		x		Planned	x		x	x
Denmark	x	x				x	x	x	x	x			x			x
Estonia	x	x				x	x	x	x	x			x			x
Finland	x	x				x	Only the country	x	x	x			x			x
France	x	x				x	with full address details	x	x	x			x		x	x
Germany	x	x				x	x	x	x	x	x	x	x			x
Greece	x	x	x		x	x		x	x				x		x	x
Hungary	x	x				x		x		x			x		x	x
Ireland	x	x				x	x	x	x				x			x
Italy	x	x				x	with full address details	x	x	x			x		with issuing authority	x
Latvia	x	x			x	x		x	x	x			x		x	x
Lithuania	x	x				x		x		x			x		x	x
Luxembourg	x	x				x	with full address details	x	x	x			x			x
Malta	x	x				x		x	x				x		x	x
Netherlands	x	x			x	x	x	x	x	x	x	x	x			x
Poland	x	x				x	with full address details	x		x			x		x	x
Portugal	x	x				x		x	x				x		x	x
Romania	x	x				x	with full address details	x	x	x			x		x	x
Slovakia	x	x			x	x	x	x	x	x			x			x
Slovenia	x	x				x		x	x	x			x		x	x
Spain	x	x				x		x	x				x		x	x
Sweden	x	x				x		x	x				x		x	x
UK	x	x				x	x	x	x	x			x			x

Table 7: Overview of the eIDAS datasets and ECI personal data requirements

4 SOLUTION 1: ELECTRONICALLY SIGNED PDF

4.1 DESCRIPTION

4.1.1 Introduction

The proposed solution is based on the use of electronic signature for signing a statement of support in a PDF format document that contains the personal data of the signatory and a specific reference to the initiative supported.

Electronic signatures are the digital equivalent of the handwritten signature on the traditional paper version of statements of support, and definitely prove the intent of a signatory to support a specific ECI. The status of electronic signatures, established 15 years ago in all Member States with the transposition of Directive 1999/93/EC, has been reinforced by Regulation (EU) 910/2014 (eIDAS Regulation). In particular, the eIDAS Regulation states that, for all Member States, qualified electronic signatures have the equivalent legal effect of a handwritten signature (Article 25). Nonetheless, the solution evaluated in this chapter is also applicable to advanced electronic signature.

This solution brings one main advantage to the system: electronic signatures usually contain data identifying the signatories as well as a link to the signed document. Thus, the use of an electronic signature provides an exclusive commitment to a specific initiative, with the added value of having the exact same value as a traditional paper-signed statement of support²³. In contrast, according to some consulted Member States' experts on the field, when an initiative is signed through the current Online Collection System, the IT system does not guarantee that the personal data collected in relation to a specific ECI is linked strictly to this specific ECI²⁴.

The possibility of signing a statement of support using an electronic signature is specifically foreseen within the current framework (Article 5, paragraph 2) under which the ECI operates. However, this feature has never been implemented in the current online collection systems. In addition, the Regulation also includes a specific reference to electronic signatures when establishing the verification procedure (Article 8, paragraph 1). Also within the reach of this solution, electronic signature could also be used by organisers in order to send the statements of support collected to the competent verifying authorities of each Member State.

²³ According to the eIDAS Regulation, only **qualified** electronic signature is strictly equivalent to paper signature. However, Article 5 of the ECI Regulation says that statements of support signed with **advanced** electronic signature is treated in the same way than a paper statement of support. This is a point to consider for clarification in case of a future revision of the ECI Regulation.

²⁴ Le Gouvernement du Grand-Duché de Luxembourg (2015) *Potential Benefits Of Electronic Signatures in The Context of European Citizen Initiatives*. p.1

4.1.2 Functional view

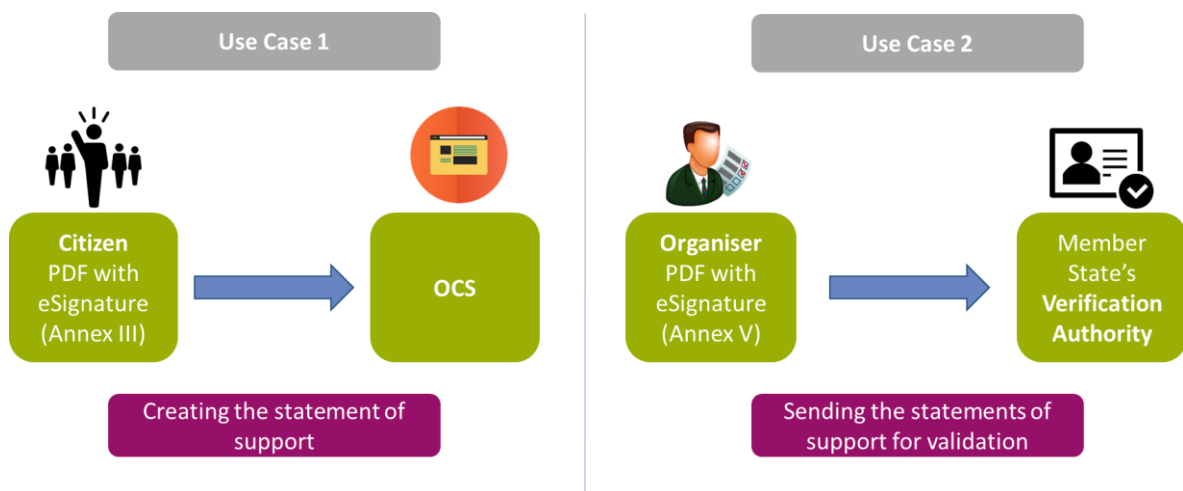


Figure 11: Different flows of information that include the use of e-signature

The two different flows of information that will include the use of e-signatures are detailed in the previous graph. On one hand, the statement of support could be submitted by uploading an electronically signed PDF document that will be stored in the OCS and validated by Member States' verifying authorities. On the other hand, when organisers of a successful initiative have to send the statements of support collected to the corresponding verification authority, they could do so electronically in a form in which the representative of the organiser's committee would include his/her e-signature.

Use Case 1: Collection of statements of support

For this business process, in combination with the verification, two alternatives exist regarding the validation of the certificate used for signing. It may be validated:

1. online during the collection phase
2. offline during the verification phase

As the first alternative implies a change in the ECI process, and therefore in the Regulation, it falls out of the scope of this chapter. Furthermore, this alternative would be very similar to the direct integration of eIDs, which is another reason for not considering it in this chapter.

This business process considers off-line signing of the PDF document. An alternative could be on-line signing: viewing the PDF (or any other format) in the browser and creating the signature in it. This variation has two draw-backs: in the first place, on-line signing is not supported in all EU Member States; in the second place this variation would entail that the user would need to (automatically) install a signature creation tool, which would cause users to be surprised. Apart from these draw-backs, such variation would be very similar (except for the validation) to solution 2: e-signature.

The architectural view with dataflows is described in the following diagram:

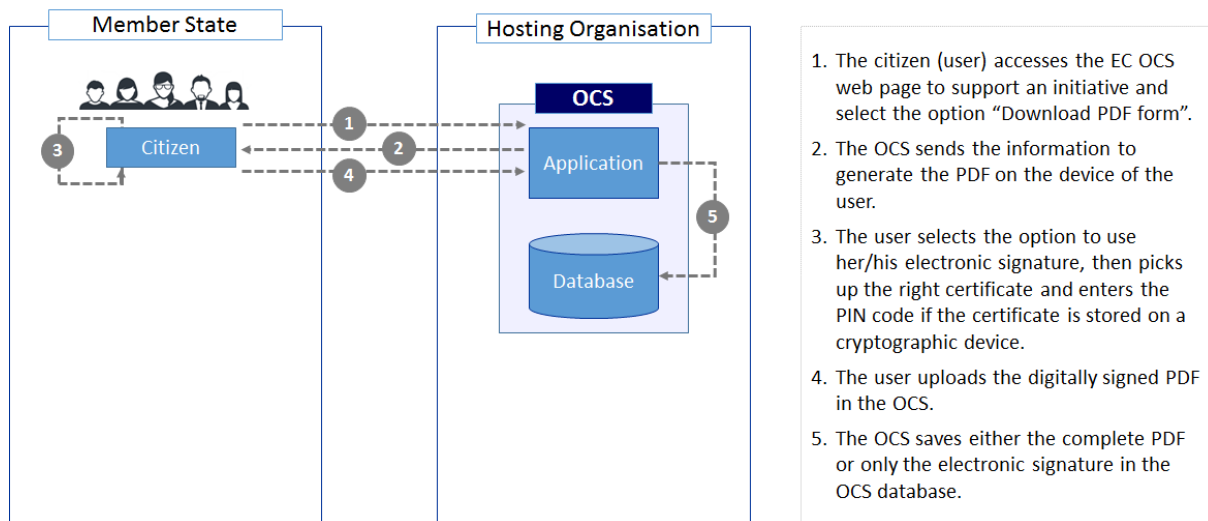


Figure 12: Architecture of electronically signed PDF document - collection phase

A detailed description of the way these elements interact is provided in "Appendix B – Solution 1: Electronically Signed PDF document", section 13.1.

This integration implies the following changes in the OCS:

- The navigation of the OCS requires changes, such as the inclusion of two buttons, for download and upload.
- When the user clicks the button "Download PDF", the OCS system will generate a PDF, with the user's data pre-filled, as far as introduced by the user.
- When the OCS receives the signed PDF, the certificate is extracted. This must be checked for validity; an elementary check is performed. The extracted certificate is stored and validated for revocation by the Member States after closing the collection phase; which is the considered use case.

Detailing the new components, the PDF manipulation library is installed in the application server together with the existing OCS software. This software is updated to support the modified navigation, as well as the inclusion of certificate validation module. The database will need an update with two additional columns, one would be the flag indicating that the support statement is produced with a signed PDF, the other one will contain the signed PDF document.

The user's PC or mobile device will need to provide support for reading PDF files. On most devices, this software is already present. A list of links to download free PDF reading software could be foreseen to ease the user experience.

Use Case 2: Verification of statements of support

Once the collection phase of an initiative comes to an end and the number of statements of support gathered has reached both the total and the national thresholds, the verification phase begins and organisers must send the statements of support to the corresponding verifying authorities. The statements of support will be sent according to Article 8 of the Regulation, using the form set out in Annex V.

A variation on this process could be thought of: instead of sending the complete statements of support, only the used certificates could be sent. However, this would require a change in the Regulation. Furthermore, the difference in size between a PDF document and a certificate is around 5 kb; if compressed this difference is even far less. One more benefit of sending the signed PDF documents is that the viewer is present in most PCs, which is not the case for certificate viewers

This procedure could also be expedited by the use of e-signature, easing the identification of the representative of the organisers committee and fostering the use of an electronic format in order to complete this phase of the ECI process. The detailed description of the use case is included in section 13.2.

4.2 LEGAL ANALYSIS

The legal analysis is threefold. First, the assessment of the ECI Regulation is developed. Then it is followed by an analysis of the aspects of eIDAS Regulation that are relevant to this solution (scope of application, e-signature standards and their legal status). Finally, an overview of the current state of e-signature across the Union is presented, based on the responses received from to the questionnaires made available to Member States representatives.

4.2.1 Overview of the ECI Regulation

As mentioned, one of the main advantages of this solution is that the use of electronic signatures is already foreseen in the ECI Regulation (Article 5, paragraph 2, and Article 8, paragraph 1). However, the research carried out so far proves that this option has not yet been developed by organisers nor national verifying authorities. At this moment of time, the OCS does not support the inclusion of e-signatures in the statements of support. This overview of the Regulation centres its attention on key aspects of the regulation that need to be assessed when attempting to implement this solution.

The following table provides a summary of the critical legal points regarding the Regulation, focusing on three main pillars: submission of statements of support (Articles 5 and 6), verification of statements of support (Article 8) and protection of personal data (Article 12). A more thorough analysis can be found in Appendix B.

Submission of statements of support	Critical Legal Point
<p><i>Article 5.1 and 5.2</i></p> <p><i>Article 6</i></p> <p><i>Annex III</i></p>	<p>Use of e-signature is foreseen in the Regulation, but this reference is made to the definitions in the Directive 1999/93/EC, now repealed by eIDAS. A new, more secure standard (qualified e-signatures) has been introduced. A modification of the wording of Article 5.2 is advisable, including a specific mention to eIDAS and the use of qualified e-signatures.</p> <p>If such certificates are to be used, Annex III will need to be modified accordingly.</p>
Verification of statements of support	Critical Legal Point
<p><i>Article 8</i></p> <p><i>Annex V</i></p>	<p>Statements of support will be sent to the corresponding verifying authorities of each Member State, following the procedure set out in Article 8. No modification is therefore</p>

	needed. Nonetheless, the form that organisers must use to submit the different statements of support for validation (Annex V) could be modified, including a specific mention to those statements of support that are based on e-signatures.
Data protection	Critical Legal Point
Article 5.3 Article 12	When statements of support are submitted via PDF documents, the data stored in the will in no case be more than the one established by each Member State in Annex III. As long as the established requirements regarding security in the OCS and data protection are met, this solution does not require additional features to be implemented in the system, or the regulation to be modified regarding this aspect.

Table 8: Legal analysis: ECI Regulation - solution 1

In essence, this analysis concludes that there are no major impediments for this solution to be carried out within the ECI regulatory framework. The submission and validation of statements of support that include e-signatures is foreseen in the Regulation, so no major roadblocks can be identified when aiming at implementing this solution. Only a modification of Annexes III and V could be taken into consideration, in order to include a more specific mention to the use of e-signature. In addition, a re-wording of Article 5, updating the reference to the use of e-signature to the qualified e-signature provided in eIDAS.

4.2.2 Comparison on the e-signature standards established in the eIDAS Regulation

Regarding the use of e-signature, the eIDAS regulation provides definitions for the different categories of e-signature available. In principle, two main categories are relevant for this solution: advanced electronic signature and qualified electronic signatures.

Given the direct effect this Regulation has on the EU territories, all Member States shall implement the established e-signature standards. The following table provides a comprehensive review on the technical features of both the advanced and the qualified electronic signature within the eIDAS Regulation:

Scope	
Art. 1: With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation: <i>“establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.”</i>	
Definitions (e-signature standards)	
Advanced electronic signatures	Qualified electronic signatures
Art. 3 (11): “advanced electronic signature” means an electronic signature which meets the requirements set out in	Art. 3 (12): “qualified electronic signature” means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified

<p>Article 26:</p> <ul style="list-style-type: none"> • <i>It is uniquely linked to the signatory;</i> • <i>It is capable of identifying the signatory;</i> • <i>It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and</i> • <i>It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.</i> 	<p><i>certificate for electronic signatures. Article 28 states that the qualified certificate shall comply with the requirements laid down in Annex I:</i></p> <ul style="list-style-type: none"> • <i>An indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;</i> • <i>A set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:</i> <ul style="list-style-type: none"> • <i>For a natural person: the person's name;</i> • <i>At least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;</i> • <i>Electronic signature validation data that corresponds to the electronic signature creation data;</i> • <i>Details of the beginning and end of the certificate's period of validity;</i> • <i>The certificate identity code, which must be unique for the qualified trust service provider;</i> • <i>The advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;</i> • <i>The location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;</i> • <i>The location of the services that can be used to enquire about the validity status of the qualified certificate;</i> • <i>(j) Where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.</i>
---	--

Table 9: Comparison of e-signature standards, eIDAS Regulation - solution 1

In light of the information presented, both categories could be suitable for implementation within this solution. Although Articles 5 and 8 of the ECI Regulation specifically mention the use of advanced e-signatures for the purpose of submitting and verifying statements of support, this solution will focus on the utilisation of qualified e-signatures, due to the enhanced security features and the highest degree of confidence in the identity of the signatory that they provide. Moreover, qualified certificates are based on Trust Lists under the control of Member States, thus providing a more reliable source for the data needed to submit a valid statement of support.

As mentioned in section 4.2.1, a modification of Annex III is to be considered, in order to include the possibility to use the e-signature for the purpose of signing a statement of support, using the qualified certificate. Moreover, Annex V could also be modified in order to allow for the use of e-

signature when organisers deliver the statements of support to the corresponding verifying authorities.

4.2.3 Analysis of the Member States' responses

The analysis of the situation of eID in the EU Member States is based on the information gathered through desk research as well as on the responses obtained from the questionnaires made available to representatives of each Member State. In total, 12 Member States shared their information:

- Austria
- Belgium
- Czech Republic
- Estonia
- Finland
- Germany
- Greece²⁵
- Luxembourg
- Netherlands
- Portugal
- Slovakia
- Spain

Key questions regarding the functioning of the ECI process and the current state of e-signature across the European Union were selected, extracting and processing the information in order to provide useful insights, aiming at assessing any possible roadblocks that this solution might face when implemented.

The responses from Member States regarding this solution can be grouped into two main areas:

- Change in the Regulation and data requirements (Annex III)
- Penetration and use of e-signature

Regarding the first aspect, the responses show that in general, Member States' verifying authorities will prefer to receive the statements of support and perform the appropriate checks for validity and duplicates, following the procedure established in the current regulatory framework. Moreover, in order to simplify the process of submitting a statement of support when implementing this solution, 30% of the consulted Member States are inclined to consider some data of Annex III as optional.

In addition, the responses from Member States received show a penetration level that is optimal for implementation, given the fact that half of the sources consulted report that e-signature certificates are issued to a majority of population, while in other countries the e-signature's popularity is growing, as more users are getting access to it. However some Member States, such as France, issue certificates to their citizens only if they are representatives of legal persons, other Member States do not issue any certificates, so in practice the citizens of these Member are excluded from using this solution.

4.3 BUSINESS ANALYSIS

The implementation of this solution brings major improvements to the Member States' verifying authorities as it simplifies the verification of the statements of support. Indeed, thanks to the

²⁵ DISCLAIMER: the information obtained from Greece was provided by a former representative that is awaiting to be replaced by the next appointed official. Therefore, the data regarding Greece cannot be considered as official.

implementation of e-signature, the certificates can be directly checked against national databases. Moreover, the qualified certificate enhances the security and accuracy of the data.

In case Member State's verifying authorities accept to consider the statements of support based on e-signatures as validated with the information contained in the e-signature certificate, this solution would also reduce the amount of data they manage as well as ease their task and the overall efficiency of the system.

Regarding the penetration level of the solution, it will have a positive impact on verifying authorities as the e-signatures certificates used in this case are usually the most widely used, increasing the confidence in the data retrieved and therefore easing the verification task.

Regarding the citizens, implementing this solution lengthens the process as more steps (downloading the PDF, uploading it, etc.) are required to finalise the submission of a valid statement of support. However, the quantity of data to be inserted manually by the user is reduced to zero as the data contained in the certificate is sufficient to validate the statements of support.

In countries where eID cards containing certificates allowing for the use of e-signatures have been issued, the impact of this solution will be higher. Despite the heterogeneous penetration of this solution across the Member States, e-signature and PDF documents are widely used across the EU and the overall penetration of this solution can thus be considered as remarkable. Indeed, the responses from the Member States show that, in many cases, the e-signature has been issued to a majority of the population. The difference between the penetration level and the actual usage of e-signatures should however also be taken into consideration when assessing the impact of this solution. The amount of people using e-signatures can indeed be significantly lower than the number of certificates delivered.

Finally, from the campaign organisers' point of view, the electronically signed PDFs do not have a major impact on the ease of use and management of both the OCS and the data they collect. However, e-signature brings added value to the delivery process of the statements of support as it serves its automation.

Moreover, as campaign organisers are considered as data controllers, under Regulation (EU) 2016/679, (repealing Directive 95/46/EC, mentioned in the ECI Regulation) during the initiative's collection phase (Article 12, paragraph 2 of the ECI Regulation), they are responsible for any damage they cause. The integrity of the data contained in e-signatures enhances the security and reduces therefore the legal risks that organisers are currently facing. This solution also helps the organisers in their planning and managing of the campaign as they are currently recommended to obtain an extra 20% statements of support in order to account for invalid ones²⁶. As the statements of support based on e-signatures provide a higher confidence in their later validation, thanks to this solutions organisers can have better idea of the number of valid statements they collected so far.

²⁶ Le Gouvernement du Grand-Duché de Luxembourg (2015) *Potential Benefits Of Electronic Signatures in The Context of European Citizen Initiatives*. p.2

The high penetration level of this solutions can also have a positive impact on campaign organisers as it might make the ECI process more attractive to the population, helping them to raise awareness and collect a larger number of statements of support. Those effects are however indirect and therefore difficult to assess.

The above-mentioned information is summarised in the following table:

Evaluation Criteria	Stakeholder	Score	Description
Ease of use	Verification Authorities	● ● ● ● ○	<ul style="list-style-type: none"> Simplification of the verification of statements of support thanks to e-signature Enhanced security and trustful data thanks to qualified certificates
	Citizens	● ● ● ○ ○	<ul style="list-style-type: none"> More steps are required to complete the submission of a valid statement of support
	Organisers	● ● ● ● ○	<ul style="list-style-type: none"> No change to the current OCS and data management Serves the automation of the statements of support delivery process
Quantity of data	Verification Authorities	● ● ● ● ○	<ul style="list-style-type: none"> Positive impact on the amount of data managed by the verification authorities in case they accept to consider the statements of support based on e-signature as validated with no additional data requirements The identity of the signatories can be established only on the e-signature certificate
	Citizens	● ● ● ○ ○	<ul style="list-style-type: none"> The quantity of data to be inserted manually is reduced to zero
	Organisers	● ● ● ● ○	<ul style="list-style-type: none"> e-signature enhances the data security and therefore reduces the legal risks campaign organisers are facing as data controllers A higher confidence in the later validation of the statements of support helps organisers in planning and managing the campaign
Penetration	Verification Authorities	● ● ● ○ ○	<ul style="list-style-type: none"> High trust in the data retrieved from e-signature (widely penetrated) eases the task of verification
	Citizens	● ● ● ○ ○	<ul style="list-style-type: none"> High penetration of e-signature and PDF documents, which are widely used across the EU
	Organisers	● ● ● ○ ○	<ul style="list-style-type: none"> The ECI process is more attractive to citizens. A higher awareness level of the ECI can lead to the collection of a larger number of statements of support

Table 10: Summary of the business analysis - e-signed PDF document

4.4 TECHNICAL ANALYSIS

The main benefit of this solution, compared with the current situation, is the fact that the signature avoids certain cases of fraud: the statements of support cannot be copied from one initiative to others without being detected. However, citizens whose nationality is from outside the EU can support initiatives, without being detected automatically. The major draw-back is the fact that the certificates used for signing are not checked on-line for their (revocation) status, so this must be checked during the verification phase.

This solution presents a good scalability: new eIDs can be introduced without any effort. Equally the maintainability is good, as no changes can be foreseen in the underlying technologies, and changes in the supported eIDs do not affect the solution. Also the ease of integration is good: many organisations have experience with the integration of the PDF manipulation libraries; as a consequence the cost/efforts are little.

Compared with the current OCS, an increase of CPU and disk usage can be foreseen, but these increases can easily be supported by modern servers.

The over-all security improves the current implementation of the OCS, not only in the already mentioned aspect of fraud prevention, also the session management is improved with the

transmission in only one http session of the statement of support, and the integrity of the data during transmission and storage is guaranteed with the signature.

The above-mentioned information is summarised in the following table:

Evaluation Criteria	Score	Description
Scalability	● ● ● ● ●	Considering that citizens are completely identified by their qualified signature, in principle the Member States' specific modules could be omitted. New eIDs are accepted without any effort.
Maintainability	● ● ● ● ●	No changes are foreseen in the TSLs and PDF/PAdES specifications.
Performance & usage of resources	● ● ● ● ○	The CPU usage will increase in an important percentage (around 70%) because of the resources needed for the certificate and signature verification, but the CPU throughput of a modern server is more than enough to support many initiatives in parallel.
Security on data storage	● ● ● ● ●	The current security measures comply with the requirements from the Regulation and the EC security policy.
Fraud prevention	● ● ● ● ○	As a statement of support is linked to a specific initiative, copying statements of support from one initiative to another is detected. The signature binds the statement of support to one specific initiative.
Security on data transmissions	● ● ● ● ○	The integrity of the data transmissions is improved, because changes in the data during the transmission can be detected as the signature would become invalid.
Session management	● ● ● ● ○	The statement of support is transmitted in one http session. The management of the relation between this session and the conformation of the support uses standard mechanisms.
Ease of integration	● ● ● ● ○	PDF manipulation libraries are easy to integrate; the creation of signatures is located outside of the OCS, therefore needing no integration effort.
Maturity	● ● ● ● ●	<ul style="list-style-type: none"> • PDF is the most commonly used standard for document exchange on the Internet • PAdES is the commonly accepted standard for signatures on PDF documents • Most PDF readers support producing advanced signatures on documents
Portability	● ● ● ● ○	Considering that this solution will be implemented in Java (back-end), and in HTML and Angular (front-end), it is portable with little effort
Cost/Efforts	● ● ● ● ○	The cost/effort estimations are around 4-5 man-months

Table 11: Summary of the technical analysis - e-signed PDF document

4.5 ASSESSMENT

Solution 1 introduces a PDF manipulation library in order to manage and store the statements of support that include e-signatures. Given the fact that those PDF documents are signed offline and uploaded on the OCS, the system does not integrate any Member State's certificate validation service. The statements of support are then not validated until they are sent to the verifying authorities once the collection phase has ended. The user interface would include a "PDF download" and a "Signed PDF upload" functions in order to allow citizens to complete the process.

The ECI Regulation already foresees the possibility of using electronic signature for supporting an initiative. Therefore, only Annexes III and V should be modified to include a more specific mention to the use of such method to submit a statement of support. Moreover, a re-wording of Article 5, updating the reference to the use of advanced electronic signature to qualified electronic signature is advisable. This would improve the trust in electronically signed documents as it would use the most reliable methods for signing. Besides, the proposed certificates (qualified electronic signatures) are compliant with the eIDAS Regulation, which is applicable to the ECI framework.

Finally, in most Member States the level of penetration of e-signature seems optimal from an implementation point of view, according to the data provided (see section 4.2.3). However, even though the availability of e-signature is high, their actual usage by citizens may remain limited.

Moreover, in some Member States such as France, hardly any qualified certificates have been issued to the citizens.

The assessment carried out through the construction of the evaluation matrix is presented in the following radar chart diagram. Detailed information about the assessment evaluation criteria can be found in Appendix B – Solution 1: Electronically signed PDF document.

Solution 1: Electronically signed PDF document

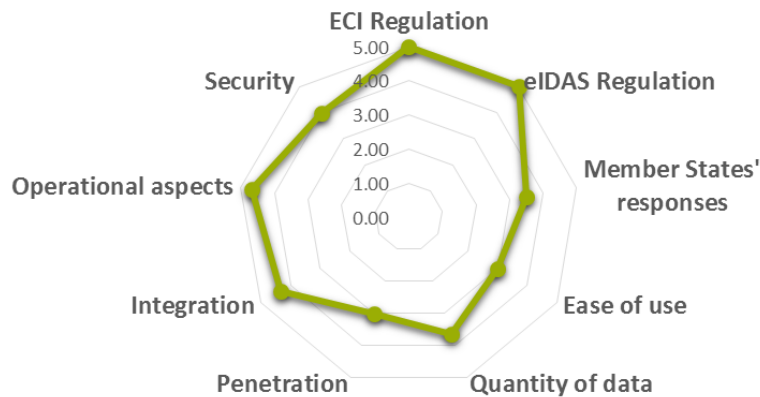


Figure 13: Assessment of solution 1

From a technical point of view, this solution achieves high scores regarding the ECI Regulation and the eIDAS Regulation (all the technical components are compliant). In addition, the integration and operational criteria are also assessed with a high punctuation marks, as no integration of Member States nodes is foreseen and the validation of the e-signature certificates is not carried out at the moment the user uploads the statement of support. Therefore, the costs associated to the implementation and maintenance of the new version of the OCS are relatively limited when compared to other solutions. Likewise, this solution will have enhanced security features, due to the limited transmission of information that is required to finalise the process.

Nonetheless, the process might require some additional time to be completed, as the user needs to download, sign and upload the PDF document. The point where this solution presents more hurdles is regarding the possibilities of reducing the quantity of data required by each country in Annex III, as the analysis of the Member State's responses has shown.

5 SOLUTION 2: INTEGRATION OF E-SIGNATURE

5.1 DESCRIPTION

5.1.1 Introduction

Solution 2 is based on the integration of electronic signature for the purpose of signing a statement of support online. The main advantage of this solution is two-fold: (1) be able to automatically verify the identity of the signatories, and (2) obtain a more specific commitment to a single initiative, thus reducing the possibility of fraud. This change in the verification process will ease the task of validation by verifying authorities, as a system for storing the indicator resulting of this activity is proposed, in order to account for the automatically validated statement of support. This would enhance the overall performance of the ECI process in general and may attract more users to support any given initiative. Therefore, the use of an electronic signature will enhance the overall performance on the OCS, simplifying the process and potentially attracting citizens into the ECI context by providing them with a more secure way to share their data and support an initiative.

There is, however, an important prerequisite for the optimal use of this solution, in particular since the Digital Signature Services (DSS) provided under CEF Digital eSignature Building Block is considered for implementation in the OCS. DSS is designed in a way that it should normally be able to handle all eIDAS-compliant e-signatures. Thus, this solution is only applicable to countries whose electronic signatures are already compliant to eIDAS.

5.1.2 Functional View

Use Case 1: Collection of statements of support

The following diagram shows the architecture and dataflows.

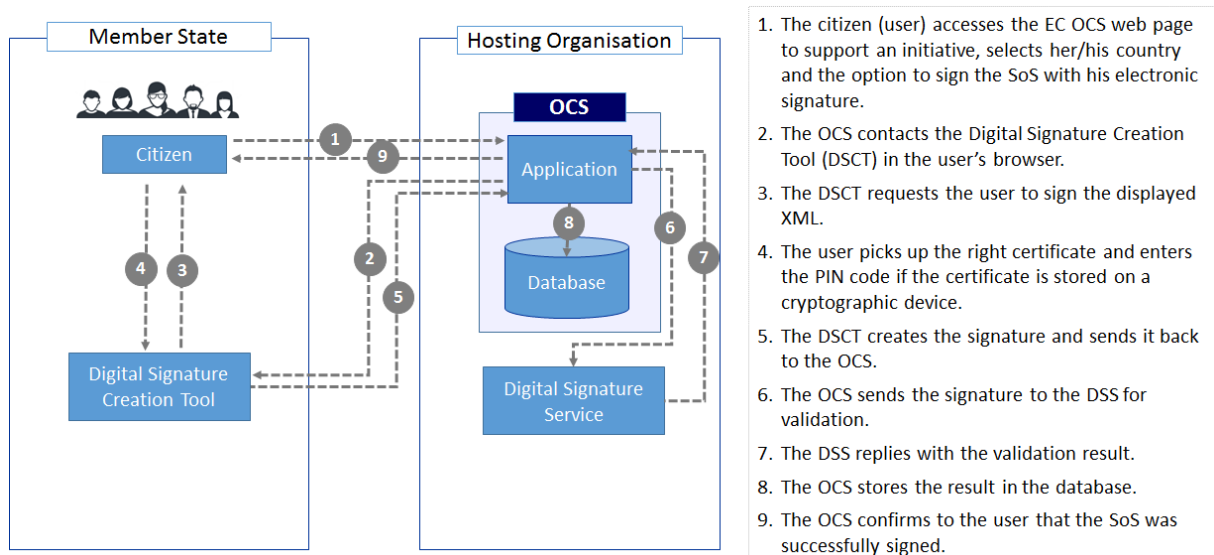


Figure 14: Architecture and dataflows for e-signature

A detailed description of the interactions between these elements is provided in section 14.1. The OCS would require the following changes:

Changes in the navigation in the OCS

The navigation in the OCS will require some changes such as the inclusion of a button to sign the statement of support online and acknowledge the validation of the signature. Additionally, the

actions corresponding to the user's clicks on these buttons must be included. These are considered minor changes.

Inclusion of DSS validation service

When the OCS receives a signed statement of support, the certificate used for signing is extracted and passed to the DSS validation service. This module verifies:

- If the certificate is qualified against the Trusted List: The check verifies if the issuer of the certificate (Certification Authority) is mentioned in the Trusted List of the citizen's Member State. More details about the Trusted List mechanism are explained in section 14.4.2, as these are relevant for the scalability.

If the certificate is valid: The checks on the validity period of the certificate entail the comparison of the current date/time with the timestamps *notBefore* and *notAfter* of the citizen's certificate. It is however more complicated to check if the certificate has been revoked or suspended: this implies consulting the corresponding "validation service" of each e-signature certificate. This validation may use the Trusted List) mechanism. The EC published a list of Trusted Lists, which provides links to the Trusted Lists of each Member State. These national trusted Lists specify all qualified CAs and for each of them the location (URL) and mechanism of the revocation validation service. As a consequence, the Member State's modules would not need to be configured with the parameters of the location and mechanism of the revocation validation service; instead it would acquire these parameters from the Trusted List.

If the certificate was issued to a natural person: In most Member States, certificates mentioned in this study are issued to only natural persons. However, in some Member States like the Netherlands and France, certificates were also issued to legal persons, which don't have the right to vote. For these Member States, the validation module should verify that the used certification policy (OID) is included in the policies for natural persons of the issuing organisations. This issue will only last for a limited period of time because since the entry into force of eIDAS, legal persons should not be issued certificates for e-signatures (they should receive certificates for e-seals instead).

Inclusion and configuration of a signature creation tool

A signature creation tool should be integrated with the OCS. Such a tool could be the signature creation service of the DSS solution published at the EC's Joinup portal²⁷. Integration of such solution implies basically three steps:

- The html page must include the code to activate the tool with the (XML) text to be signed as a parameter
- The tool must be configured to view the text to sign and to produce a XAdES signature. This tool (and also other tools) is designed to allow multiple signature formats. Since normal users have insufficient knowledge of signature formats and their implications, the signature tool must be configured to hide this complexity for the end user.

²⁷ <https://joinup.ec.europa.eu/software/sd-dss/release/all>

- The tool and the page must be prepared to transmit the signature produced by the tool to the browser.

The user's PC or mobile device needs to support Web navigation. This software is usually installed by default and is used in the current version of the OCS. The Member State's validation service (CRL or OCSP) will also remain unchanged.

For certificates not held by the citizen, like the Austrian and Estonian mobile solutions, the user is redirected to the corresponding signature creation service. In this case, the link to the service includes the data to be signed. The reply by the creation service is sent through the browser to the OCS application. In this case, the validation is not required anymore, as these services only allow the creation of signatures with valid and qualified certificates.

As only qualified signatures are allowed, the Member States may consider not requiring the full dataset as specified in Annex III, as the citizen is identified by his data in the certificate.

Use Case2: Verification of statements of support

The business process verification of statements of support is equal to the process described in 4.1.2, but replacing the signed PDF documents with signed XML structures. The viewer is also replaced by any XAdES signature viewer.

5.2 LEGAL ANALYSIS

5.2.1 Overview of the ECI Regulation

The following table provides a summary of the critical legal points regarding the ECI regulation, focusing on three main pillars: submission of statements of support (Articles 5 and 6), verification of statements of support (Article 8) and protection of personal data (Article 12). A more thorough analysis can be found in section 14.2.1.

Submission of statements of support	Critical Legal Point
<p><i>Article 5.1 and 5.2</i></p> <p><i>Article 6</i></p> <p><i>Annex III</i></p>	<p>The use of e-signature is foreseen in the Regulation, but this reference is made to the definitions in the Directive 1999/93/EC, now repealed by eIDAS. A new, more secure standard (qualified e-signatures) has been introduced. A modification of the wording of Article 5.2 is advisable, including a specific mention to eIDAS and the use of qualified e-signatures.</p> <p>If such certificates are to be used Annex III will need to be modified accordingly.</p>
Verification of statements of support	Critical Legal Point
<p><i>Article 8</i></p> <p><i>Annex V</i></p>	<p>Validation of the information contained in the certificates would be performed when the statement of support is submitted. Therefore, Article 8 should be modified in order to include the new procedure for verification and the flagging of the information that has been already validated.</p> <p>Nevertheless, in case verifying authorities wish to perform further checks, the statements of support would still be delivered following in accordance to Article 8.1.1.</p>
Data protection	Critical Legal Point
<p><i>Article 5.3</i></p> <p><i>Article 12</i></p>	<p>When statements of support are submitted via this solution, the data stored will in no case be more than the one established by each Member State in Annex III.</p> <p>As long as the established requirements regarding security in the OCS and data protection are met, this solution does not require additional features to be implemented in the system, or the regulation to be modified regarding this aspect.</p>

Table 12: Legal analysis: ECI Regulation - solution 2

5.2.2 Analysis of the eIDAS Regulation

Regarding the use of e-signature eIDAS establishes a whole new regulatory framework, substituting previous directives.

This solution foresees the possibility to allow the use of qualified electronic signatures, given the fact that they provide the highest level of assurance regarding the identity of the person signing an

initiative. The eIDAS Regulation also establishes an unambiguous legal value for electronic signatures that is different for the various categories.

All Member States shall follow this standard, as the eIDAS Regulation has direct effect on their territories. The following table provide a comprehensive review on qualified electronic signatures, trust services and the legal value of e-signatures:

Scope	
<p>Art. 1: With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:</p> <p><i>“Establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.”</i></p>	
Definitions (e-signature and trust services)	
Qualified electronic signatures	Trust services
<p>Art. 3 (12): <i>‘qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. Article 28 states that the qualified certificate shall comply with the requirements laid down in Annex I:</i></p> <ul style="list-style-type: none"> • <i>an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;</i> • <i>a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:</i> <ul style="list-style-type: none"> • <i>for a natural person: the person’s name;</i> • <i>at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;</i> • <i>electronic signature validation data that corresponds to the electronic signature creation data;</i> • <i>details of the beginning and end of the certificate’s period of validity;</i> • <i>the certificate identity code, which must be unique for the qualified trust service provider;</i> • <i>the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;</i> • <i>the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;</i> • <i>the location of the services that can be used to enquire about the validity status of the qualified certificate;</i> <p><i>(j) Where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.</i></p>	<p>Art. 3(16): ‘trust service’ means an electronic service normally provided for remuneration which consists of:</p> <ul style="list-style-type: none"> (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services; <p>Art.3 (17): ‘qualified trust service’ means a trust service that meets the applicable requirements laid down in this Regulation</p> <p>Art. 3(19): ‘trust service provider’ means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;</p> <p>(20) ‘qualified trust service provider’ means a trust service provider who provides one or more qualified trust services and is gr</p> <p>Art. 22.1: Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.;</p> <p>2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.</p> <p>3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.</p>

Table 13: Legal analysis, eIDAS Regulation - solution 2

As mentioned, this solution foresees the use of qualified signatures, since they provide the highest degree of confidence in the identity of the person signing the statement of support. Besides, qualified certificates are only issued by qualified service providers, who are under strict control of Member States through national laws and trusted lists. Therefore, these are ideal tools to be integrated into the OCS, providing secured and trustworthy data that verifying authorities will be able to validate without further checks.

The research carried out has concluded that all Member States have published and updated trusted lists, and therefore qualified electronic signatures are issued all across the EU. The fact that the selected eIDs are already penetrated across Member States increases the probability of a successful implementation and the establishment of a new procedure to create statements of support that is secure and compliant with the eIDAS Regulation. However some Member States do not issue signature certificates to their complete population, e.g. France and the Netherlands only issue certificates to representatives of legal persons; other countries have other limitations to issuing certificates to their population.

Besides, the legal value granted to qualified electronic signatures provides safe grounds for organisers and verifying authorities to comply with their task with no legal risks associated.

5.2.3 Analysis of Member State responses

The analysis of the situation of eID in the EU Member States is based on the information gathered through desk research as well as on the responses obtained from the questionnaires made available to representatives of each Member State. In total, 12 Member States shared their information:

- Austria
- Belgium
- Czech Republic
- Estonia
- Finland
- Germany
- Greece²⁸
- Luxembourg
- Netherlands
- Portugal
- Slovakia
- Spain

As mentioned, a key component of the proposed solution is the corresponding flag that will be stored in the OCS as a sign that the statement of support is produced when data is retrieved from the certificate. Regarding the format and security features of the flag were presented, obtaining in general positive responses.

The responses received can be summarised under two main points:

- Member State generally agree to implement the responses from Member States. Especially, the possibility of flagging the data retrieved from the certificates has received great support from the sources consulted. However, it is important to note the reluctance of certain Member States towards the use of the e-signature certificates, mainly due to the costs that would need to be incurred.

²⁸ DISCLAIMER: the information obtained from Greece was provided by a former representative that is awaiting to be replaced by the next appointed official. Therefore, the data regarding Greece cannot be considered as official.

- The penetration level of e-signature seems to be optimal for implementation in several Member States, while other countries do not provide such figures but show a positive growing trend in the penetration of e-signature. Both these facts are proof of the suitability of the implementation of this solution.

5.3 BUSINESS ANALYSIS

This solution, similar in many points to solution 1, brings the added value of an on-the-spot validation of the statement of support when the users sign the statement of support in the ECI entry point. This fact could certainly ease the validation task from the corresponding verifying authorities, as the data will be flagged indicating that it was already validated. Furthermore, the fact that qualified certificates are the ones to be used, and that such certificates are under supervision of Member States through Trusted, increases the possibility that no further verification is required in order to validate statements of support collected from this source. As mentioned, the penetration level would provide a suitable implementation, as e-signature is issued to a major part of the population in several countries, while the number of certificates used is growing in many others.

In addition, the possibility to sign online would improve the submission procedure from a user experience perspective, as the time devoted to complete the process will be reduced compared to the current situation and the scenario of solution 1. Provided that users are allowed to use their qualified certificates, the amount of data that they need to introduce manually will be reduced to zero.

Regarding organisers, no major changes are expected in the way they manage the statements of support gathered. Given the enhanced security features of the qualified certificates, the legal risk they face as data controller would be reduced. Besides, they could benefit from the overall improvement of the OCS and the possibility to attract a larger number of citizens to the ECI tool.

The above-mentioned information are summarised in the following table:

Evaluation Criteria	Stakeholder	Score	Description
Ease of use	Verification Authorities	● ● ● ● ●	<ul style="list-style-type: none"> Simplification of the verification of statements of support thanks to e-signature Enhanced security and trustful data thanks to qualified certificates
	Citizens	● ● ● ● ●	<ul style="list-style-type: none"> Reduction of the time devoted to submit a valid statement of support. The process would be more user-friendly.
	Organisers	● ● ● ○ ○	<ul style="list-style-type: none"> No change in the current way data is managed Serves the automation of the statements of support delivery process
Quantity of data	Verification Authorities	● ● ● ● ○	<ul style="list-style-type: none"> Positive impact on the amount of data managed by the verification authorities in case they accept to consider the statements of support based on e-signature as validated with no additional data. Only checks for duplicates would be necessary in case authorities wish to perform any further validation.
	Citizens	● ● ● ● ●	<ul style="list-style-type: none"> The quantity of data to be inserted manually is reduced to zero
	Organisers	● ● ● ● ○	<ul style="list-style-type: none"> e-signature enhances the data security and therefore reduces the legal risks campaign organisers are facing as data controllers A higher confidence in the later validation of the statements of support helps organisers in planning and managing the campaign
Penetration	Verification Authorities	● ● ● ○ ○	<ul style="list-style-type: none"> On-the-spot validation and high trust in the data retrieved from e-signature (widely penetrated) eases the task of verification.
	Citizens	● ● ○ ○ ○	<ul style="list-style-type: none"> Although all countries issue qualified certificates, only 50% of the MS consulted can assure that e-signature is issued to the majority of adult population. Some MS have indicated a growing trend regarding its use.
	Organisers	● ● ● ○ ○	<ul style="list-style-type: none"> The ECI process would be attractive to citizens. A higher awareness level of the ECI can lead to the collection of a larger number of statements of support

Table 14: Summary of the business analysis - e-signature

5.4 TECHNICAL ANALYSIS

The main benefit of this solution, compared with the current situation, is the fact that the used eID is validated, thus releasing the verifying authorities of the burden to check the statement of support. Another benefit can be found as the signature avoids certain cases of fraud: the statements of support cannot be copied from one initiative to others without being detected. However, citizens whose nationality is from outside the EU can support initiatives, without being detected automatically.

This solution presents a good scalability: new eIDs can be introduced without any effort. However, the maintainability may suffer from introduction of new eIDs, if those affect the connection with the DSS solution.

Compared with the current OCS, an increase of CPU and disk usage can be foreseen, but these increases can easily be supported by modern servers.

The over-all security improves the current implementation of the OCS, not only in the already mentioned aspect of fraud prevention, also the session management is improved with the transmission of the statement of support in only one http session, and the integrity of the data during transmission and storage is guaranteed with the signature.

The above-mentioned information is summarised in the following table:

Evaluation Criteria	Score	Description
Scalability	● ● ● ● ●	The e-signature service provided by the Commission (DSS) is scalable as it performs the validation of the signature itself and does not rely on Member State's specific modules to validate the certificate or extract the user's data.
Maintainability	● ● ● ● ○	The maintainability is considered moderate due to the number of Member States' modules and their complexity.
Performance & usage of resources	● ● ● ● ○	The CPU usage will increase in an important percentage, but the throughput of a modern server is more than enough to support several initiatives in parallel.
Security on data storage	● ● ● ● ○	The current security measures comply with the requirements from the Regulation and the EC security policy.
Fraud prevention	● ● ● ○ ○	Fraud prevention is improved, as citizens can't support on behalf of other persons. Statements of support cannot be copied from one initiative to others. However, most eIDs don't include the nationality of the citizen, so citizens from outside the EU could vote.
Security on data transmissions	● ● ● ● ○	This solution provides a secure transmission mechanism, the data transmissions between the OCS and the citizen use a secure channel (SSL or TLS).
Session management	● ● ● ● ○	The statement of support is transmitted in one http session. The management of the relation between this session and the conformation of the support uses standard mechanisms.
Ease of integration	● ● ● ○ ○	The 28 Member States' specific modules are complex due to the validation and extraction functions.
Maturity	● ● ● ○ ○	e-signature has been present in the EU for some years and the penetration level is optimal for implementation. On the other hand, the DSS solution has been recently developed, and might still face some operational issues.
Portability	● ● ● ● ●	The solution with Java is portable with little effort. Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different appservers.
Cost/Efforts	● ● ● ○ ○	The cost/effort estimations are around 12 man-months.

Table 15: Summary of the technical analysis - e-signature

5.5 ASSESSMENT

This solution foresees the use of e-signature, but in contrast with solution 1, the OCS would establish a connection with the Member State's e-signature creation tool and a seamless online validation would be performed by the DSS module. For that purpose, the OCS would redirect the user towards the homepage of the e-signature creation tool (this page should hide the complexity of the national implementation in case multiple e-signature solutions are available in a Member State). Then, the OCS will be performing the validation of the e-signature and it will extract the information contained in the e-signature certificates. The data will be flagged and stored in the OCS, as proof of the automatic validation carried out when retrieving the information from the certificate.

A revision of the ECI Regulation is required to achieve a successful implementation of the proposed integration of online e-signature into the ECI process. Firstly, Article 8 should be modified to include the new verification method (extraction and validation of the information in the certificates carried out by the OCS) and the indicator proving that the information that has been already validated. Secondly, Annex III should be amended to include the e-signature method, with the subsequent reduction of the data requirement that it entails.

The assessment and scoring performed for this solution is summarised in the following diagram that groups the main assessment criteria in order to provide a general view of the results obtained. Detailed information about the assessment evaluation criteria can be found in Appendix C – Solution 2: e-signature.

Solution 2: e-signature integration

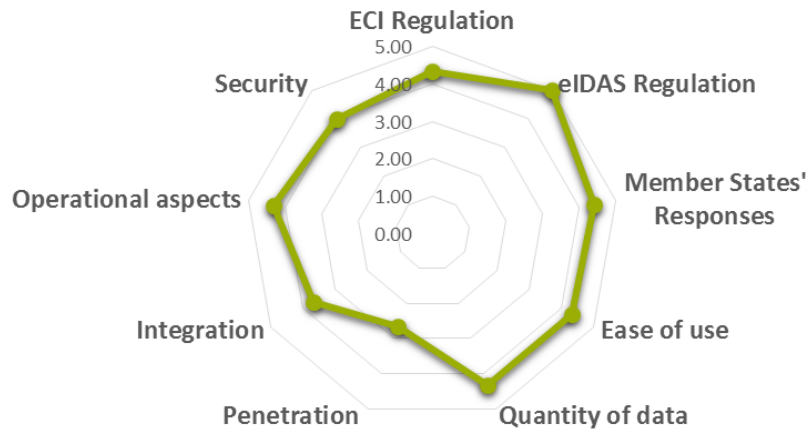


Figure 15: Assessment of solution 2

As shown in the graph, this solution presents generally high scores in all the legal criteria, especially regarding the responses obtained from Member States, who showed a favourable opinion towards the flagging system and the automatic validation. Given the reduction of data required and the improvement in the process to submit the statement of support, this solution is also assigned high scores in ease of use and quantity of data.

Nevertheless, and even though the technology is in a suitable penetration level, integrating and maintaining the new custom-built will be complex and costly. Therefore, the integration and operational aspects of this solution are ranked with the lowest scores.

5.6 COMPARISON OF SOLUTIONS 1 AND 2

The following table provides a comparison of the SWOT analysis between solution 1 and solution 2.

	Solution 1: Electronically signed PDF	Solution 2: Integration of e-signature
Strengths	<ul style="list-style-type: none"> • Ease of implementation • Penetration of the solution (PDF and e-signature) • Presence in the Regulation: e-signature is mentioned in Article 5 and 8 as part of the ECI process • Data security: information related to eSignature is stored in the PDF, therefore more difficult to be tampered or used for other purposes • The solution is mature (it has already been put in place in Member States, does not need to be connected to eIDAS) • No shift of responsibility regarding the online validation of statements of support. Members States remain the responsible 	<ul style="list-style-type: none"> • Ease of use: the process will be simple and short to complete • Data quality for organisers: data will be retrieved from national eID databases • Automatic validation: data retrieved from a Member State eID service will be flagged • Penetration of the solution: eID is available to a significant percentage of the population • Scalability and maintainability (if DSS is used for implementation of the solution)
Weaknesses	<ul style="list-style-type: none"> • Ease of use: the statement of support has to be downloaded, signed offline, and then uploaded: it would create a more time-consuming process • No automatic validation is foreseen, as statements of support will be stored and sent to the verification authorities after the collection phase • Regulation mentions advanced electronic signatures, however qualified electronics signatures are preferable 	<ul style="list-style-type: none"> • Costly integration: This solution would require the integration with every single Member State eID nodes
Opportunities	<ul style="list-style-type: none"> • Verification authorities could consider statements of support as pre-validated • Simplification of Annex III: inclusion of a form that only requires the use of eSignature • Possibility to use qualified electronic signatures (enhanced LoA) 	<ul style="list-style-type: none"> • A change in Regulation will lead to a simplification of the process • This solution will raise awareness / commitment / consciousness towards the ECI tool • Possibility to shift the responsibility of the online validation of statements of support to the EC
Threats	<ul style="list-style-type: none"> • If Annex III is not modified, the user will have to complete the additional data manually, adding time and complexity to the process. • A modification of Annex III and Annex V is advisable. 	<ul style="list-style-type: none"> • This solution foresees a change in Regulation, therefore making it difficult to get all the Member States on board • eIDAS (alternative connection approach) is going to be in place by 2018

Figure 16: SWOT analysis of solutions 1 and 2

As those two solutions can be easily compared from several points of view, the table hereunder provides a comparison based on a set of the identified evaluation criteria.

Evaluation Criteria	Solution 1	Solution 2	
ECI Regulation	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	Solution 2 requires an amendment of Article 8 and a modification of Annex III while no change in the regulation is necessary for the implementation of solution 1.
eIDAS Regulation	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	Both solutions comply with the eIDAS Regulation
Member States' responses	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	The comparison of the responses is not relevant as the questions focused on different aspects of each solution.
Ease of use	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	Compared to solution 1, the data retrieved from e-signature is trustful and the validation task is therefore easier. Moreover, the process for the citizens is smooth and user-friendly.
Quantity of data	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	By implementing solution 2, the quantity of data to be inserted by the user is reduced to zero and the number of statements of support to be validated by verification authorities is reduced while for solution 1, they still need to verify the identity of signatories.
Penetration	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	Only 50% of the Member States consulted can assure that eSignature is issued to the majority of adult population. However, for both solutions, the data is retrieved from trustworthy sources, easing the task of verification authorities
Operational aspects	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	The two solution are mainly similar regarding operational aspects
Security	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	The two solutions are mainly similar regarding security
Integration	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●	Solution 2 is more complex to integrate than solution 1

Table 16: Comparison of solutions 1 and 2

6 SOLUTION 3: DIRECT INTEGRATION OF EID

6.1 DESCRIPTION

6.1.1 Introduction

This solution consists in the integration of the most widely used national eID solution into the OCS: direct integration of eID. Within this scenario, the personal data requested for a signatory to support an initiative will be retrieved from the national eID database of each Member State.

This chapter discusses the advantages and drawbacks of direct integration; the OCS will be extended with the modules required to access the user's eID, validate it and extract the data from it. The data will be retrieved from Member State's eID portal and will be stored in the OCS with a flag²⁹ or indicator that will account for the statement of support that have been already validated.

Once the collection phase comes to an end, verifying authorities will be delivered the corresponding set of statement of support, separating all the different kinds. This solution proposes certain regulatory changes in order to give the eID integration a more solid and stable legal ground.

6.1.2 Functional View

Use Case 1: Collection of statements of support

The architecture and dataflows of this solution is shown in the following diagram.

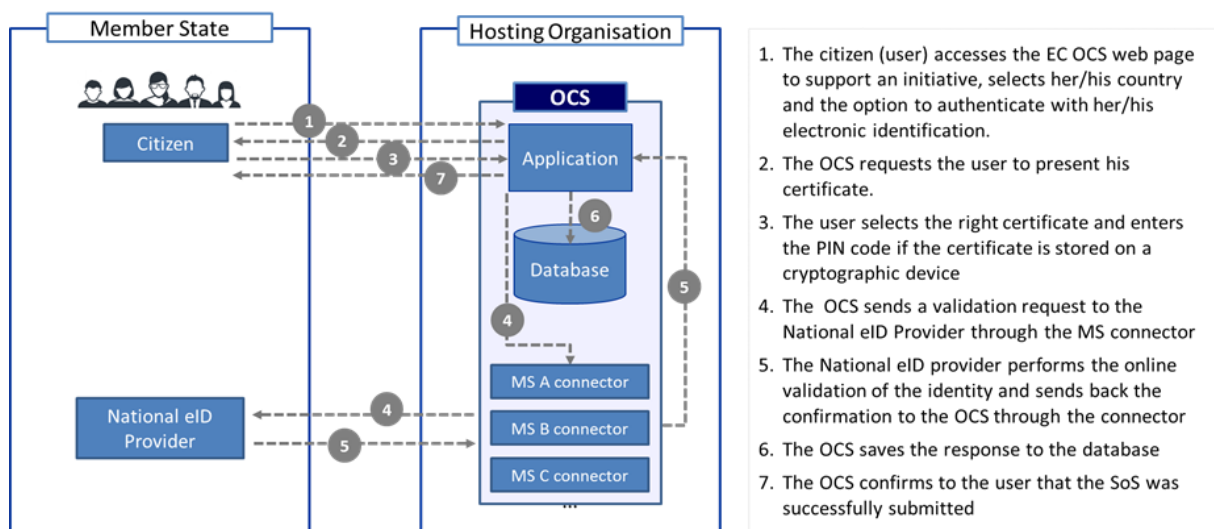


Figure 17: Architecture and dataflows for direct integration of eID

A detailed description of the interactions between these elements is provided in section 15.1.

The OCS is updated to support the changed navigation and the included Member States specific modules, one for each supported Member State, in charge of:

²⁹ In case Member States do not accept to modify Annex III and reduce the personal data requirements, an alternative option would be to take advantage of this solution to retrieve the data coming from the national register of natural persons. This data would then be used to partially fill the statement of support (as read-only fields). The user would then enter manually the missing data. This alternative provides advantages to the verifying authorities, which thus benefits from trustworthy data, as well as to the users as it shortens the submission process and increases the user-friendliness of the system.

- The validation of the used certificate
- The extraction of the data from the certificate

When the OCS receives a certificate, this certificate is passed to a first validation module, before passing it to the corresponding Member State specific module. This validation module is in charge of the first validation of the used certificate. This validation entails the checks that:

- The certificate is already valid, comparing the timestamp `notBefore` with the current date/time.
- The certificate is not expired, comparing the timestamp `notAfter` with the current date/time.
- The Country (“C”) of issuer of the certificate is in the list of 28 EU Member States.
- The issuer of the certificate is mentioned in the national Trust List (TSL); this means that the issuer is a qualified authentication service provider.

The Member State specific module checks:

- If the certificate is valid: if the certificate has been revoked or suspended as is determined by consulting the corresponding “validation service” of each Member State for the certificate used in the authentication. Two parameters are important for this validation: the method to be used and the location where this method should be applied; these parameters are explained in section 15.4.1.
- If the certificate was issued to a natural person: In most Member States, certificates mentioned in this study are issued to natural persons. However, in some Member States, like France and the Netherlands, certificates are also issued to legal persons, which do not have the right to vote. For those Member States, the validation module should verify that the used certification policy (OID) is included in the policies for natural persons of the issuing organisations.

The extraction of the data is not straightforward due to the heterogeneous formats of the citizen’s data. Apart from the changes in the OCS, other changes can be found in the database: it will be updated to add two columns: the first one is the indication (flag) that the statement of support is achieved using an eID, the second one would be the user’s eID. If a qualified eID has been used for authentication, the user will not need introduce the data specified in Annex III manually, in case Member States decide to accept such statements of support.

The user’s PC or mobile device will need to support web navigation. On most devices this software is already present, and it is also used in the current version of OCS. The Member State validation service (CRL or OCSP) will not suffer any changes as these services exist and are already available on the Internet.

Use Case 2: Verification of statements of support

Once the collection phase comes to an end, verifying authorities will be delivered the corresponding set of statements of support, separating all the different kinds. This solution proposes certain regulatory and technical changes in order to give the eID integration a more solid and stable legal ground.

The verification of statements of support with directly integrated eIDs is the same as with signed PDF documents, 4.1.2, except for the format of these statements: instead of the PDFs, now the certificates are sent.

6.2 LEGAL ANALYSIS

6.2.1 Overview of the ECI Regulation

The following table provides a summary of the critical legal points regarding the ECI regulation, focusing on three main pillars: submission of statements of support (Articles 5 and 6), verification of statements of support (Article 8) and protection of personal data (Article 12). A more thorough analysis can be found in section 15.2.1.

Submission of statements of support	Critical Legal Point
<i>Article 5.1 and 5.2</i>	A specific mention to the use of eID when submitting a statement of support is advisable.
<i>Article 6</i>	In order to comply with Article 6.1, paragraph 2, the model for creating the statement of support should be modified to include only the data present in the eID.
<i>Annex III</i>	A marker or flag will be added in the database to indicate that certain data fields were retrieved from the eID, and can be considered as automatically validated.
	Accordingly, a modification in Annex III is recommended, in order to include the possibility to use eID for the purpose of submitting a statement of support.
Verification of statements of support	Critical Legal Point
<i>Article 8</i>	It is recommended to amend Article 8 in order to include a specific mention to the automatic validation of data coming from eIDs, with a flag/indicator that will account for the statements of support that have been already validated.
<i>Annex V</i>	The Annex III should also be modified by adding a specific criteria for the statements of support submitted via eID. Those should be sent to the country issuing the eID, in case national authorities wish to carry out further validation or checks for duplicates.
Data protection	Critical Legal Point
<i>Article 5.3</i>	In accordance to Article 5.3, this solution does not require citizens to provide any extra information, and only the relevant data for validating the identity of a signatory will be stored in the OCS.
<i>Article 12</i>	Article 12 does not have to be modified, as the data stored is still protected against unlawful uses or losses, as long as the OCS complies with the security requirements stated in Article 6.4.
	This solution can therefore be implemented with no change in the Regulation regarding data protection.

Table 17: Legal analysis: ECI Regulation - solution 3

In brief, certain aspects of the Regulation require a modification in order to make the proposed integration of eID fits the regulatory framework under which the ECI operates:

- Regarding the collection phase (Article 5), a specific mention to the possibility of using eID to submit a statement of support is recommended. The model for creating the statements of support will be modified (Article 6.1, paragraph 2), as well as the Annex III.
- As far as the verification of the statements of support is concerned, Article 8 should be amended, adding a mention to the automatic validation when using eID for creating a statement of support. The Annex III should also be modified in order to include a specific criteria for the statements of support submitted via eID.
- Finally, no change in the Regulation is required regarding data protection (Article 12).

6.2.2 Analysis of the Member States' responses

The analysis of the situation of eID in the EU Member States is based on the information gathered through desk research as well as on the responses obtained from the questionnaires made available to representatives of each Member State. In total, 12 Member States shared their information:

- Austria
- Belgium
- Czech Republic
- Estonia
- Finland
- Germany
- Greece³⁰
- Luxembourg
- Netherlands
- Portugal
- Slovakia
- Spain

The information gathered from Member States can be summarised in two main points:

- In general, Member States share a positive opinion towards an implementation of an eID connection to the OCS. Positive feedback has been received regarding the flagging system and the possibility to consider certain data requirements from Annex III as optional, in case the Regulation was to be modified, enabling validation with the data present on the signatory eID.
- Legal and technical constraints such as being able to distinguish natural and legal persons through the eID solution and having in place an interactive verification that allows for automatic validation of the data can be overcome. This aspect signals the desirability and feasibility of the implementation of this solution from the perspective of the Member State's national legislation point of view.

³⁰ DISCLAIMER: the information obtained from Greece was provided by a former representative that is awaiting to be replaced by the next appointed official. Therefore, the data regarding Greece cannot be considered as official.

6.3 BUSINESS ANALYSIS

Implementing the direct integration of national eIDs adds a major advantage to Member State's verifying authorities. It indeed eases the verification of statements of support as the integrity and correctness the signatory's data is guaranteed by the national eID database. Verifying authorities receive the statements of support with a flag signalling the ones already validated. They thus only need to validate the ones signed in paper or submitted online through the OCS, by entering the data manually. The impact on the amount of data to be managed is thus positive for the Member States. The direct integration of eID therefore eases the task of verification by creating an automatic procedure to validate an important portion of the statements of support received, in a shorter period of time, leading to an enhancement of the overall performance of the system. However, if verifying authorities still want to, additional post-verification and checks for duplicates can still be carried out. Verifying authorities will benefit the most from the use of eID as the information is retrieved from the official eID database and can thus be trusted.

The user interface of the ECI entry point will be slightly modified, in the page where the citizen is supposed to fill in the data, to include a support button for the use of eID. On condition that the users are in possession of a valid eID tool and the specific hardware that might be required, citizens will benefit from a more secure system and a less time consuming process, as retrieving the data from the eID is faster than typing it in. Verifying authorities should be able to recognise the identity of the signatories from the data retrieved from the eIDs, as this information is normally consistent with the one stored in the national registries. Therefore, the successful implementation of the proposed solution should not require inputting any additional data. The quantity of data for this solution could be adjusted and redefined with a change of the Annex III, making sure that the data stored in the national eIDs would be sufficient to support an initiative. Consequently, the quantity of data inserted by the user should be reduced to zero. With the direct integration of eID, the user will not have to introduce much sensitive data into the OCS in order to support an initiative, making the system more attractive and user-friendly.

No significant impact on complexity is expected for campaign organisers as the statements of support submitted by means of eID will be sent to the corresponding Member State's verifying authorities following the procedure detailed in Article 8 of the Regulation, as it is done now. Implementing this solution may help organisers internally in their planning and assessment tasks as statements of support based on eIDs would give higher confidence in their latter validation. However, the positive impact on the quantity of data managed by organisers would not be significant. The data retrieved from the eID enhances the security of the overall system, therefore reducing the legal risk organisers are facing, as they are considered as data controllers, responsible for any damage they cause. This may attract more concerned citizens to become organisers and campaign for any given cause. However, this effect might be indirect and is difficult to assess.

The above-mentioned information are summarised in the following table:

Evaluation Criteria	Stakeholder	Score	Description
Ease of use	Verification Authorities	● ● ● ● ● ○	<ul style="list-style-type: none"> Reduced number of statements of support requiring verification once the collection phase has ended.
	Citizens	● ● ● ● ● ○	<ul style="list-style-type: none"> more secure system and a less time consuming process on condition that the users have a valid eID tool and the specific hardware that might be required.
	Organisers	● ● ● ● ● ●	<ul style="list-style-type: none"> No difference is expected in the way organisers manage the collection and delivery of statements of support.
Quantity of data	Verification Authorities	● ● ● ● ● ○	<ul style="list-style-type: none"> This solution creates an important reduction in the number of statements of support that need to be validated.
	Citizens	● ● ● ● ● ●	<ul style="list-style-type: none"> The quantity of data to be input is reduced to zero.
	Organisers	● ● ● ● ● ○	<ul style="list-style-type: none"> It gives organisers a more clear idea on the actual number of valid statements of support collected.
Penetration	Verification Authorities	● ● ● ● ● ○	<ul style="list-style-type: none"> The information is retrieved from the highest penetrated national eID database and can thus be trusted.
	Citizens	● ● ● ● ● ○	<ul style="list-style-type: none"> The user do not have to introduce sensitive data into the OCS.
	Organisers	● ● ● ● ● ○	<ul style="list-style-type: none"> The legal risk faced as data controller is reduced (this effect is indirect and difficult to assess).

Table 18: Summary of the business analysis – Direct integration of eID

6.4 TECHNICAL ANALYSIS

The main benefit of this solution, compared with the current situation, is the fact that the used eID is validated, thus releasing the verifying authorities of the burden to check the statement of support. Another benefit can be found as the signature avoids certain cases of fraud: it is harder to support twice the same initiative, although not impossible. Also, citizens whose nationality is from outside the EU can support initiatives, without being detected automatically in most Member States.

This solution presents a very difficult scalability: new eIDs cannot be introduced without any effort. Also, the maintainability will suffer from introduction of new eIDs or changes in their specifications: such changes will likely cause the Member State-specific modules to be adapted.

Compared with the current OCS, an increase of CPU and disk usage can be foreseen, but these increases can easily be supported by modern servers.

The over-all security improves the current implementation of the OCS: the session management is improved with the transmission of the statement of support in only one http session.

The above-mentioned information is summarised in the following table:

Evaluation Criteria	Score	Description
Scalability	● ○ ○ ○ ○	Scalability issues exist in the Member State's specific modules. New eIDs would require new MS's specific modules; new MS would also require new modules.
Maintainability	● ○ ○ ○ ○	Any change in the specifications of any of the eIDs or their validation method would require a change in its corresponding module.
Performance & usage of resources	● ● ● ● ○	A modern server can produce and verify some 50 signatures per second, which is 80.000 signatures per day. If CPU usage would be a bottle-neck, several servers could be used in parallel.
Security on data storage	● ● ● ● ○	The current security measures comply with the requirements from the Regulation and the EC security policy. The normal back-up procedure guarantees the recovery of statements of support in case of accidental loss.
Fraud prevention	● ● ● ○ ○	Fraud prevention is improved, as citizens cannot submit a statement of support on behalf of other persons. However, as most eIDs don't include the nationality of the citizen, so additional rules must be implemented to prevent citizens from non-EU countries to vote in case they have an eID card/token from their EU country of residence.
Security on data transmissions	● ● ● ● ○	The confidentiality is guaranteed due to the usage of SSL or TLS channel for data transmissions between the OCS and the citizen
Session management	● ● ● ● ○	The management of the relation between this session and the conformation of the support uses standard mechanisms.
Ease of integration	● ○ ○ ○ ○	The MS's specific modules are complex due to the validation and extraction functions, and there are 28 such modules.
Maturity	● ● ● ● ○	eIDs are available, or will soon be implemented, in all Member States.
Portability	● ● ● ○ ○	Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different application servers.
Cost/Efforts	● ○ ○ ○ ○	Estimations are between 20 to 25 man-months.

Table 19: Summary of the technical analysis – Direct integration of eID

6.5 ASSESSMENT

The implementation of solution 3 would require to include a wide number of changes in the ECI current way of functioning. Firstly, the OCS is connected to every Member State eID node in order to allow the transmission of data and validation of the statements of support. This requires to integrate a connection with every country's node that is in charge of checking their validity. Conversely, the task of verifying authorities is significantly eased when the validation of the certificates is performed by the OCS.

In pursuance of the mentioned modifications, a revision of several Articles of the ECI Regulation is needed. Article 5 should include a specific reference to the use of eID for the purpose of submitting a statement of support. The model for creating the statements of support (described in Article 5) should be modified too. Furthermore, Article 8 should also be modified to allow and accept the on-the-spot verification of the signatories' identity that would be carried out by the system. A subsequent modification of Annex III is also foreseen, in order to amend the data requirements when eID is used for the purpose of submitting a statement of support, as users only provide the data contained in their eID certificates. This Annex should also be modified by adding a specific criteria for the statements of support submitted via eID.

An in-depth assessment of this solution is presented in the following diagram. Detailed information about the assessment evaluation criteria can be found in Appendix D – Solution 3: Direct integration of eID.

Solution 3- Direct Integration of eID

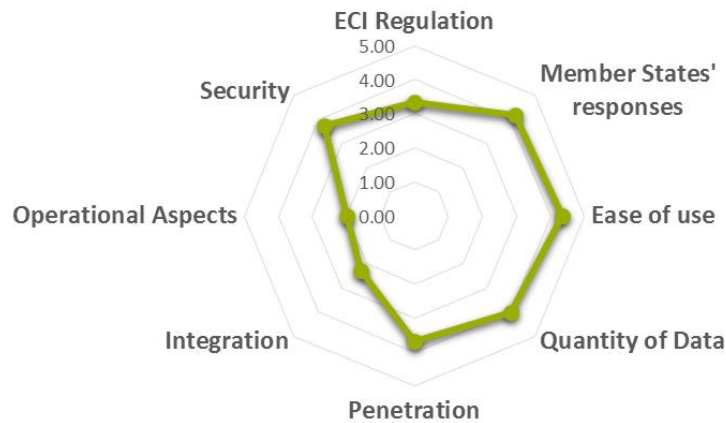


Figure 18: Assessment of solution 3

Although this solution significantly enhances the user experience and reduces the quantity of data to be inserted by signatories, this solution requires great efforts to be implemented. These hampering factors, associated to the integration and maintenance of the different Member State's nodes, are the cause of the low score of the integration and operational criteria.

Consequently, a reform on the ECI Regulation is required, although the specific changes to be incorporated are not significant. Still, according to the responses to the questionnaires, a positive attitude towards the proposed flagging system is shared by most Member States and, according to the data provided, eID schemes all over the EU are largely suitable for integration with the OCS.

7 SOLUTION 4: INTEGRATION WITH THE EIDAS FRAMEWORK

7.1 DESCRIPTION

7.1.1 Introduction

Solution 4 also foresees integration of eID into the OCS, but in this case with an indirect approach. Instead of including all the different Member States' nodes as required in the direct integration of eID (solution 3), implementing this solution requires to establish a connection with the eIDAS framework of interoperability.

Regulation (EU) 910/2014 (eIDAS Regulation)³¹ creates a European internal market for eTS - namely electronic signature, electronic seal, time stamp, electronic delivery service and website authentication - by ensuring that they will work across borders and have the same legal status as traditional paper based procedures.

The eIDAS framework provides a secure environment for Member States to receive and send personal data, with a high degree of confidence in the identity of the citizen involved in any electronic transaction. Therefore, this is an ideal solution for the integration of eID in the context of the ECI, as verifying authorities will be able to trust the data retrieved from any other Member State. A new feature of eIDAS, which will be introduced in the near future, is worth highlighting: the powers of representation and mandates. This feature will allow citizens to authorise other citizens to perform certain actions on their behalf. Allowing powers of representation and mandates in the ECI Regulation would definitely increase the reach of this solution.

The eIDAS Regulation is complemented by several implementing regulations, such as Commission Implementing Decision (EU) 2015/296 of 24 February 2015 on procedural arrangements for Member States cooperation on eID, Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework, Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means and Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification.

7.1.2 Functional view

Use Case 1: Collection of statements of support

In this context, the solution will be based on a connection between the OCS and the eIDAS framework, retrieving data once the citizen has used his/her eID certificate. The process to submit a statement of support using this solution will be very similar to solution 3, direct integration of eID (see section 6.1.1).

The architecture and dataflows of this solution are shown in the following diagram.

³¹ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>

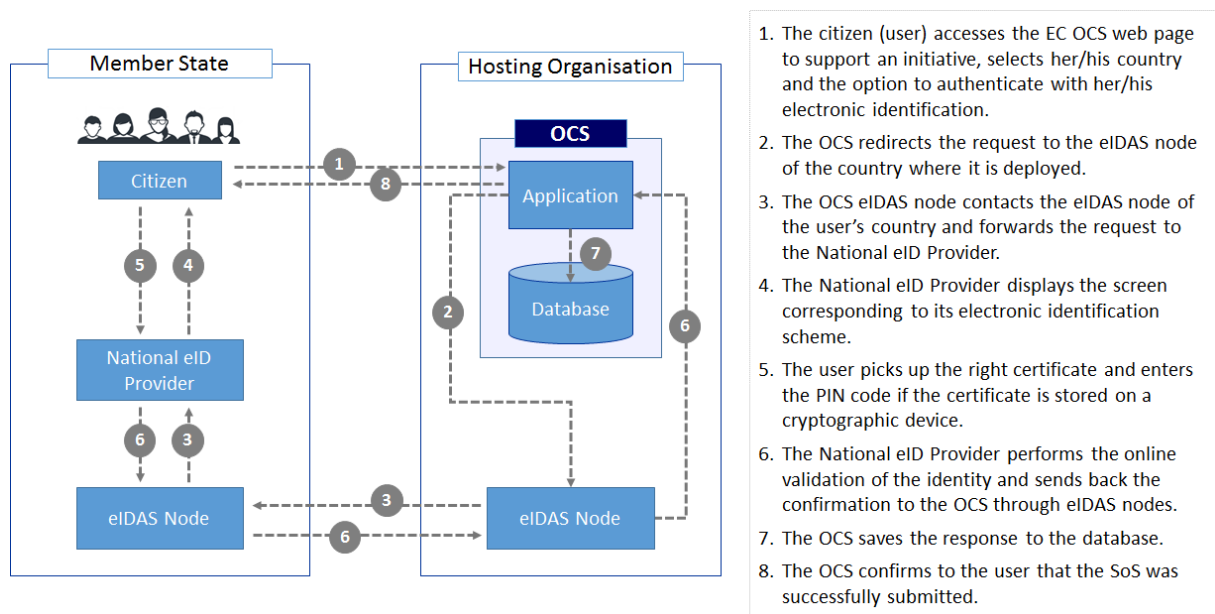


Figure 19: Architecture and dataflows of eIDAS integration

The OCS is updated to support the changed navigation and the inclusion of the eIDAS connection module. This module is part of the CEF eID building block³², as an example integrated in its test application module "SP".

Changes in the navigation in the OCS

The navigation in the OCS need some changes such as the inclusion of a button to retrieve the user's eID, and some code to process the response. These are considered as minor changes.

Inclusion of the eIDAS connection

The eIDAS connection modules must be configured in order to retrieve the citizen's data. This entails in the first place the required quality of the eID, which is recommended to be substantial, and the data to be requested: these are recommended to be the minimum dataset: name, surname, date of birth and personal identification number. When the nationality would be included, this should also be requested.

When the OCS receives the response from the EC eIDAS node, it checks if the response was signed by the eIDAS node of the Member State where the OCS is located (MS eIDAS node in the diagram). The eIDAS connection module to be integrated in the OCS verifies if the certificate used for signing the response from the MS eIDAS node is equal to the stored eIDAS certificate for this node.

There is no need to check that the data supplied by eIDAS belongs to a natural person. Indeed, as the request includes attributes for natural persons, the eIDAS transaction would fail if those attributes were not delivered. As the check on validity of the user's eID is performed by the Member State, it does not need to be performed by the OCS. Before inserting the data received from eIDAS into the database, for most countries the personal Identifier should be transformed to the citizen number: the prefix of 2 characters is stored as the nationality, and one more prefixed character is eliminated. For some countries, this is not the citizens number, e.g. in Germany and Greece no citizen number

³² This building block can be found at <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+v1.1>

exists; in others like Austria the citizen number is encrypted before being delivered to the eIDAS platform.

For traceability reasons, it would be recommendable to store the eIDAS responses in the OCS database. With this storage solution, any fraud could be easily be detected, because:

- The time-stamp of the eIDAS response must be coherent with the timestamp in the database; even though a difference of a few seconds may exist.
- The time-stamp in the response should be different from time-stamps in all other responses in all initiatives.
- The user's data in the response must match the user's data in the database.

An update of the database is required to add three columns: the first indicating that the statement of support is produced with the eIDAS platform, the second with the achieved level of assurance and the third containing the response from the EC eIDAS node.

The user's PC or mobile device will need to support web navigation. This software is installed by default on most devices, and is already needed in the current version of the OCS.

Use Case 2: Verification of statements of support

The verification of statements of support been produced using the eIDAS platform is very similar to the same process of the solution 1, as described in section 4.1.2. The only difference is that instead of signed PDF documents, the rows of the database are sent as a CSV (comma separated list) file, for easy importation in spreadsheets or databases.

7.2 LEGAL ANALYSIS

7.2.1 Overview of the ECI Regulation

From a legal point of view, the direct integration of eID and the integration with the eIDAS Framework are mainly similar. However, whereas for solution 3 a mention to the use of eID in the Regulation should be taken into consideration, for solution 4 a specific mention to the eIDAS Regulation is advisable.

The following table provides a summary of the critical legal points regarding the ECI regulation, focusing on three main pillars: submission of statements of support (Articles 5 and 6), verification of statements of support (Article 8) and protection of personal data (Article 12). A more thorough analysis can be found in section 16.2.1.

Submission of statements of support	Critical Legal Point
<p><i>Article 5.1 and 5.2</i></p> <p><i>Article 6</i></p> <p><i>Annex III</i></p>	<p>A specific mention to the use of eID when submitting a statement of support should be taken into consideration.</p> <p>As this solution foresees the access to the eIDAS network for the request of information to identify signatories, a specific mention to the eIDAS Regulation would be advisable to provide the proper legal basis for its implementation.</p> <p>A marker or flag will be added in the database to indicate that certain data fields were retrieved from the eID, and</p>

	<p>can be considered as automatically validated.</p> <p>In order to comply with Article 6.1, paragraph 2, the model for creating the statement of support should be modified to include only the data shared by the corresponding MS within the eIDAS framework.</p> <p>To comply with the last condition of Article 6.4, a modification in Annex III is recommended, in order to include the possibility to use eID for the purpose of submitting a statement of support and accepting the submission of a statement of support with the data shared by the corresponding Member State through eIDAS.</p>
Verification of statements of support	Critical Legal Point
<p><i>Article 8</i></p> <p><i>Annex V</i></p>	<p>It is recommended to modify Article 8 in order to include a specific mention to the automatic validation of the data through eIDAS, with a flag/indicator that will account for the statements of support that have been already validated.</p> <p>The Annex III should be modified by adding a specific criteria for the statements of support submitted via eID. Those should be sent to the country issuing the eID, in case national authorities wish to carry out further validation or checks for duplicates.</p>
Data protection	Critical Legal Point
<p><i>Article 5.3</i></p> <p><i>Article 12</i></p>	<p>In accordance to Article 5.3, this solution does not require citizens to provide any extra information, and only the relevant data for validating the identity of a signatory will be stored in the OCS.</p> <p>As the eIDAS Regulation only foresees sharing the Minimum and Optional data sets, additional data to the one requested by Member State is in use for the purpose of supporting an initiative.</p> <p>Article 12 do not have to be modified, as the data stored is still protected against unlawful uses or losses, as long as the OCS complies with the security requirements stated in Article 6.1, 6.3 and 6.4,</p> <p>This solution can be implemented with no change in the Regulation regarding data protection.</p>

Table 20: Legal analysis: ECI Regulation - solution 4

To summarise, for this solution as well some aspects of the ECI Regulation require a modification in order to make the proposed integration with eIDAS to be clearly binding within the regulatory framework that governs the ECI process:

- For the submission of statements of support, a specific mention to the possibility to use eID and connect to the national databases through eIDAS in order to submit a statement of support is necessary. Accordingly, a modification in Annex III is desirable to establish that statements of support only require the data shared by Member States through eIDAS to be successfully validated as well as to include the possibility to use eID for the purpose of submitting a statement of support. Moreover, the model for creating the statements of support will also need to be modified (Article 6.1, paragraph 2).
- Regarding the verification of statements of support, a modification of Article 8 is advisable in order to include a specific mention to the automatic validation of the data retrieved through eIDAS. Moreover, a modification of Annex III is also to be considered, to further establish that statements of support containing eID data shall be sent to the Member State where the eID was issued.
- Finally, similarly to solution 3, no change in the Regulation is required regarding data protection (Article 12).

7.2.2 Overview of the eIDAS Regulation

The following table provides a summary of the critical legal points regarding the eIDAS regulation, focusing on scope (Articles 1 and 2), internal market principle (Article 4), data protection (Article 5) and assurance level (Article 8). A more thorough analysis can be found in section 16.2.2.

Scope	Critical Legal Point
<p>Article 1</p> <p>Article 2</p>	<p><i>To implement a connection with eIDAS, it is important to establish clear rules and conditions to achieve interoperability among all the Member States, so eID solutions across the Union can be trusted and successfully connected to the OCS.</i></p> <p><i>Trust services play a main role in electronic identification and in the authentication and retrieval of data required in this solution, in order to establish a connection system that becomes a reliable source for verifying authorities so they can consider statements of support as automatically validated.</i></p> <p><i>Integrating eID solutions into the OCS via the eIDAS network would not result in a closed system determined by national regulations, but the ECI Regulation at EU level. Therefore, eIDAS Regulation is directly applicable to solution 4.</i></p>
Internal market principle	Critical Legal Point
<p>Article 4</p>	<p>Once this solution is implemented, the OCS will be fully integrated into the Digital Single Market, and will be able to make request for specific data to the corresponding service</p>

	providers (national eID databases).
Data protection	Critical Legal Point
<i>Article 5</i>	Article 12 of the ECI Regulation establishes a set of security features that the OCS should have in order to ensure only lawful use of personal data. As such conditions will be met, implementing this solution is in line with both the ECI and the eIDAS Regulation.
Assurance level	Critical Legal Point
<i>Article 8</i>	The eID solutions need to be consistent with the substantial or high level of assurance to establish a reliable eID connection that is able to provide trustworthy data.

Table 21: Legal analysis: eIDAS Regulation - solution 4

In summary, this solution fits in the eIDAS regulation from the scope perspective as the interoperability, trust and legal conditions are met. Moreover, from the internal market principle, this solution will be able to make request for specific data to the corresponding service providers. This solution also fulfils the data protection conditions, therefore being in line with both the ECI and the eIDAS Regulation. Finally, as the eID tools proposed for the integration are based on national eID schemes, they are catalogued as substantial or high as regards the Assurance Level.

7.2.3 Analysis of the Member States' responses

Together with the general eID responses analysed for solution 3 (See section 6.2.2), the analysis of solution 4 is complemented with three specific questions related to the current state of eIDAS and what information would Member States be willing to share, in order to provide a clear view of the AS IS situation of eIDAS across the European Union.

- The possibility of having the nationality as part of the data shared by eIDAS is of key importance for the implementation of this solution, given the fact that nationality is one of the primary requirements for a citizen to support an initiative within the ECI framework. However, the responses obtained from the consulted Member States show that there is no agreement on sharing nationality for this purpose, although half of the countries show a positive opinion towards this possibility.
- Moreover, the Unique Identifier, which is key when aiming at identifying the identity of the signatory, is not sufficient for the verification of statements of support. However, for some of the countries, the minimum data say would be sufficient to establish the identity of a citizen.
- Finally, almost all Member States who stated they would only require the Minimum Set of Data to validate a statement of support, are not favourable to the possibility of sharing the Place of Birth and Residence, as they consider those data as not necessary to establish the identity of a citizen, with the data retrieved via eIDAS.

7.3 BUSINESS ANALYSIS

Similarly to the direct integration of eID, the statements of support submitted using this solution can be considered as automatically validated and Member States' verifying authorities will still receive the statements of support to give them the possibility to perform additional checks. This automatic validation is made possible thanks to the system of flags that can be added to the information coming from trusted sources. The integration of eIDAS and the ECI online platform increases the quality of online statements of support and therefore eases the task of validation. Regarding the quantity of data, the impact on verifying authorities is similar to solution 3, the only difference between the two solutions being how the connection to the eID database is established. The impact of the penetration level/awareness is also similar to the one for the direct integration of eID into the OCS.

From the citizens' point of view, the ease of use of this solution is similar to the one of solution 3. The process is as easy to access and complete, despite the redirection to the home country eID website before retrieving the data. Moreover, the vast majority of the Member States consulted are able to establish the identity of the citizens with the Minimum Set of Data. Therefore, this solution departs from the assumption that statements of support containing the Minimum Set of Data, established in the eIDAS Regulation, are automatically validated as verifying authorities are able to establish the identity of the signatories. Consequently, the quantity of data to be inserted by the user is reduced to zero. The impact of the penetration level/awareness on the citizens is similar to the one for the direct integration of eID into the OCS. Besides, as eIDAS also provides supports to any type of eID, including (reinforced) username / password schemes, the penetration level for this solution is significantly higher than the direct integration of eID. However, the full potential of this solution will not be a reality until all the nodes are operational and therefore totally interoperable.

The fact that the data is retrieved directly (solution 3) or via eIDAS does not make a difference for campaign organisers, neither from the ease of use or from the quantity of data perspectives. The impact of the penetration level/awareness is similar to the one for the direct integration of eID into the OCS.

The above-mentioned information are summarised in the following table:

Evaluation Criteria	Stakeholder	Score	Description
Ease of use	Verification Authorities	● ● ● ● ○	<ul style="list-style-type: none"> Reduced number of statements of support requiring verification once the collection phase has ended.
	Citizens	● ● ● ● ○	<ul style="list-style-type: none"> Smooth, user friendly and fast process on condition that the users have a valid eID tool and the specific hardware that might be required.
	Organisers	● ● ● ● ●	<ul style="list-style-type: none"> No difference is expected in the way organisers manage the collection and delivery of statements of support.
Quantity of data	Verification Authorities	● ● ● ● ○	<ul style="list-style-type: none"> This solution creates an important reduction in the number of statements of support that need to be validated.
	Citizens	● ● ● ● ●	<ul style="list-style-type: none"> The quantity of data to be input is reduced to zero.
	Organisers	● ● ● ○ ○	<ul style="list-style-type: none"> It gives organisers a more clear idea on the actual number of valid statements of support collected.
Penetration	Verification Authorities	● ● ● ● ○	<ul style="list-style-type: none"> The information is retrieved from the highest penetrated national eID database and can thus be trusted and the verification task is easier.
	Citizens	● ● ● ● ○	<ul style="list-style-type: none"> The user do not have to introduce sensitive data into the OCS.
	Organisers	● ● ● ○ ○	<ul style="list-style-type: none"> The legal risk faced as data controller is reduced (this effect is indirect and difficult to assess).

Table 22: Summary of the business analysis – Integration with the eIDAS framework

7.4 TECHNICAL ANALYSIS

The main benefit of this solution, compared with the current situation, is the fact that the used eID is validated, thus releasing the verifying authorities of the burden to check the statement of support. Another benefit can be found as the eIDAS integration avoids certain cases of fraud: it is harder to support twice the same initiative, although not impossible using eIDs from different Member States. Also, citizens whose nationality is from outside the EU can support initiatives, without being detected automatically. These two points would be improved if the nationality of the citizen would be included in the eIDAS specifications.

This solution presents a good scalability: new eIDs can be introduced without any effort. Also, the maintainability is good: no changes can be foreseen which affect the eIDAS integration into the OCS.

Compared with the current OCS, an increase of CPU and disk usage can be foreseen, but these increases can easily be supported by modern servers.

The over-all security improves the current implementation of the OCS: the session management is improved with the transmission in only one http session of the statement of support, and the integrity of the data transmission and storage are protected with signatures.

The above-mentioned information is summarised in the following table:

Evaluation Criteria	Score	Description
Scalability	● ● ● ● ●	New eIDs or new Member States would not require any change in the OCS.
Maintainability	● ● ● ● ●	Any change in the specifications of any of the eIDs or their validation method does not require any change in the OCS.
Performance & usage of resources	● ● ● ● ○	Performance tests in the STORK project have shown that a modern server can produce and verify some 50 signatures per second, which is 4M signatures per day.
Security on data storage	● ● ● ● ○	The current security measures comply with the requirements from the Regulation and the EC security policy.
Fraud prevention	● ● ● ○ ○	Fraud prevention is improved, as citizens can't support on behalf of other persons. However, statements of support could be copied from one initiative to others, with difficult detection of such fraud.
Security on data transmissions	● ● ● ● ○	The eIDAS network guarantees confidentiality with encryption, and the integrity with signatures.
Session management	● ● ● ● ●	The statement of support is transmitted in one http session. The management of the relation between this session and the conformation of the support uses standard mechanisms.
Ease of integration	● ● ● ● ●	Only one module with a simple API is to be integrated.
Maturity	● ● ○ ○ ○	Only one eID has been pre-notified (Germany), while several others will be this year.
Portability	● ● ● ● ●	Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different application servers.
Cost/Efforts	● ● ● ● ●	The cost/effort estimations are around 3 man-months

Table 23: Summary of the technical analysis – Integration with the eIDAS framework

7.5 ASSESSMENT

Despite the similarities that solutions 3 and 4 might present, implementing solution 4 seems more feasible from a technical point of view. In this case, the OCS is only integrated into the eIDAS node, granting a safe connection to Member State's eID access points. Consequently, the corresponding Member State eIDAS node is the one performing the tasks of validation and extraction of the information contained in the eID certificates.

As proposed, a modification of the ECI Regulation is to be considered, aiming at including a specific reference to the use of eID (Article 5) and the eIDAS network as a connection pathway to grant an automatic validation of the statements of support. Moreover, the model for creating the statements of support (described in Article 5) should also need be modified. A modification of Article 8 is also required, in order to allow and accept the on-the-spot verification of the signatories' identity that would be carried out by the system through eIDAS. Moreover, Annex III should be modified in order to amend the data requirements when authentication through eIDAS is used for the purpose of submitting a statement of support, as only the minimum dataset provided by eIDAS (name, surname, date of birth and personal identification number) will be available. It is also necessary to obtain the agreement from the eIDAS expert group to use one of the eIDAS custom field to store the nationality of the signatory as this information is required for the validation of the business rules. Finally, all notified eID schemes are granted a substantial or high level of assurance, and therefore are compatible with the eIDAS Regulation, as this solution is based on qualified service providers and Trust Lists.

The following diagram provides a thorough assessment of this solution. Detailed information about the assessment evaluation criteria can be found in Appendix E – Solution 4: Integration with the eIDAS Framework.

Solution 4- eIDAS Integration

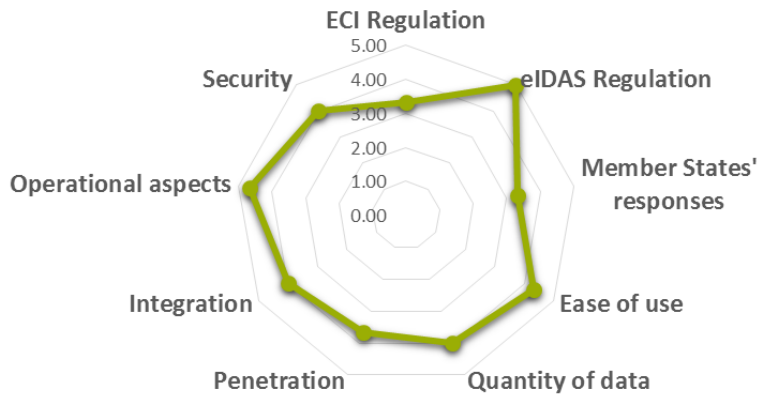


Figure 20: Assessment of solution 4

As this diagram shows, the solution presents high scores regarding its integration and functional aspects, due to the simplification of the integration that the eIDAS network provides. Besides, it is also translated in a remarkable reduction of the quantity of data to be inserted into the OCS, as users are only required to connect to their eID access point and validate the transmission of the data. This improvement of the process to submit a statement of support is also reflected in our assessment, as the criterion of ease of use is assigned a noteworthy score. The enhance security provided by eIDAS is also to be noted.

Nevertheless, the responses from Member States are not so clear regarding this solution, mainly because of the production and testing phase that the majority of Member States is immersed in at the moment this report is elaborated. The fact that an important part of them were not able to provide a clear answer regarding the data that will finally be sent to the OCS is a proof of the construction stage that eIDAS is facing. Nonetheless, this solution should be fully operational by September 2018.

7.6 COMPARISON OF SOLUTIONS 3 AND 4

The following table provides a comparison of the SWOT analysis between solution 3 and solution 4.

	Solution 3: Direct integration of eID	Solution 4: Integration with the eIDAS framework
Strengths	<ul style="list-style-type: none"> Ease of use: the process will be simple and short to complete Data quality for organisers: data will be retrieved from national eID databases Automatic validation: data retrieved from a Member State eID service will be flagged Penetration of the solution: eID is available to a significant percentage of the population Ease of implementation / integration (connection to eIDAS node) 	<ul style="list-style-type: none"> Ease of use: Solution 4 offers a better ease of use than solution 1 Improved quality of data thanks to qualified electronic signatures Less data to be input by the user Penetration of the solution: Qualified electronic signature is available in almost all Member States (eIDAS compliance). Automatic/Direct validation
Weaknesses	<ul style="list-style-type: none"> Maturity of the solution: all Member States will not be compliant with eIDAS until 2018 Possible lack of data, not all Member States seem to be willing to share all the necessary data (minimum Data Set, optional Data Set, sectorial information) 	<ul style="list-style-type: none"> Costly implementation: A connection with every Member State node is needed Maintainability (many nodes, at least one per Member State).
Opportunities	<ul style="list-style-type: none"> A change in Regulation will lead to a simplification of the process This solution will raise awareness / commitment / consciousness towards the ECI tool Possibility to shift the responsibility of the online validation of statements of support to the EC 	<ul style="list-style-type: none"> Simplification of the process Possibility to shift the responsibility of the online validation of statements of support to the EC
Threats	<ul style="list-style-type: none"> This solution foresees a change in Regulation, therefore making it difficult to get all the Member States on board 	<ul style="list-style-type: none"> Change in Regulation (to include Qualified Electronic Signatures as the only ones allowed)

Figure 21: SWOT analysis of solutions 3 and 4

As those two solutions can be easily compared from several points of view, the table hereunder provides a comparison based on a set of the identified evaluation criteria.

Evaluation Criteria	Solution 5	Solution 6	
Data Privacy	● ● ● ● ● ●	● ● ○ ○ ○ ○	EU Login presents security features that make it a suitable solution for a potential integration with the OCS. On the contrary, regarding Facebook's privacy agreement, there is a concern regarding what specific information would Facebook have access to, and where this would be stored, regarding citizens and also organisers of any given initiative.
Member States' responses	n/a	n/a	n/a
Ease of use	● ● ○ ○ ○ ○	● ● ● ○ ○ ○	For both solutions, once the user authorises his/her data to be retrieved, the statement of support is automatically prefilled. There is a possibility to remove the CAPTCHA before submitting the statement of support.
Quantity of data	● ○ ○ ○ ○ ○	● ● ○ ○ ○ ○	With EU Login external accounts, the user still need to enter most of the data manually. With Facebook, the quantity of data to be input by the user depends on each Member State's requirements.
Penetration	● ○ ○ ○ ○ ○	● ● ● ○ ○ ○	While EU Login is a fairly new service that is not currently used by a significant part of the EU population, Facebook has a penetration rate of 39.5% in Europe.
Operational aspects	● ● ● ● ● ⚡	● ● ● ● ● ⚡	The operational aspects are similar for both solutions.
Security	● ● ● ○ ○ ○	● ● ● ○ ○ ○	Both solutions presents similar score regarding security.
Integration	● ● ● ● ● ●	● ● ● ● ● ●	Both solution are easy to integrate, mature, portable and don't require a lot of effort or cost to be implemented.

Table 24: Comparison of solutions 3 and 4

8 SOLUTION 5: PREFILLING USER'S DATA WITH EU LOGIN

8.1 DESCRIPTION

8.1.1 Introduction

This chapter analyses a complementing tool for prefilling a statement of support: EU Login (formerly known as ECAS-ID). This solution is used to retrieve data from the user's account, easing the process of supporting an ECI by reducing the amount of data to be filled manually by the user and possibly by removing the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).

The European Commission Authentication Service (ECAS) has recently been merged into the EU Login, a broader identification system that aims at providing access to every online service provided by the EU, with one single account. Researchers, experts, EU officials, and citizens in general can manage their data and performing a wide number of tasks through one single platform, increasing operational efficiency and making the access to online public services user-friendlier.

The EU login foresees several ways to log into the account:

- By creating a new account with a username and a password
- By accessing with a former ECAS account credentials
- By linking EU Login with social media platforms (Twitter, Facebook and Google +)

Besides, the traditional password authentication, once the user has access to the EU account, he/she can set up two-step authentication method, choosing among a wide range of alternatives:

- PIN Code through the ECAS mobile Application
- QR Code through the ECAS mobile Application
- SMS sent to his/her phone number (only possible if the user saved a valid phone number in the EU Account)
- Using a Token that provides an authentication method (i.e., an USB)
- Using his/her eID (STORK pilot)

In this context, the EU Login could be used as a complementary tool for prefilling some data of the statement of support. Thanks to this solution, the user has the possibility to retrieve some of his data saved in his EU Login account to automatically prefill part of his statement of support, easing the supporting process. Although the EU Login feature is restricted to EC applications due to EC policies, it is taken into account as a technical possibility.

As for most of the authentication methods mentioned here above, there is no way to certify the accuracy of the user's data, the prefilled fields of the statement of support should remain editable. This way, the user can still bring modifications and adapt some data if necessary. The user then fills in the data not present in the EU Login account manually.

However, it should be mentioned that severe limitations for the use of EU Login in external applications were reported by the persons in charge of this tool. Thus, this solution would only be applicable for the EC OCS, but not for any other implementation of OCS by third parties.

The reason for this limitation is that the EC does not operate yet a full eIDAS node, which could be used by a client application. The eIDAS connectivity is actually built into EU Login. Consequently, using the EC eIDAS node would actually mean using EU Login for eID authentication. This has the following limitations:

- EU Login can only be used by systems that are owned and operated by EU institutions. This is due to political, legal and financial aspects.
- EU Login cannot be used by external parties without prior registration.
- EU Login is currently not organised to provide authentication services to external applications on a large scale.
- EU Login is not capable to limit authentication options to eID only.

However, this idea could lead to another possible solution, "3 bis": Integration via an embedded eIDAS Connector. This solution relies on the usage of the eIDAS network for eID authentication, just like solution 3. But instead of using an EC eIDAS node, the integration would happen via an eIDAS connector that is embedded in the solution. In other words, the application would use an eIDAS connectivity library. An OCS deployment with that solution would behave like a standalone eIDAS node, and would be able to consume eID authentications from other nodes. After evaluation, this solution 3 bis was discarded because it would require Member States to define a new connector for each OCS willing to connect to EU Login.

Despite these considerations, the solution is fully described in this chapter in order to perform an exhaustive analysis as per initial request.

8.1.2 Functional View

Use Case 1: Collection of statements of support

The architecture and dataflows are represented in the following diagram.

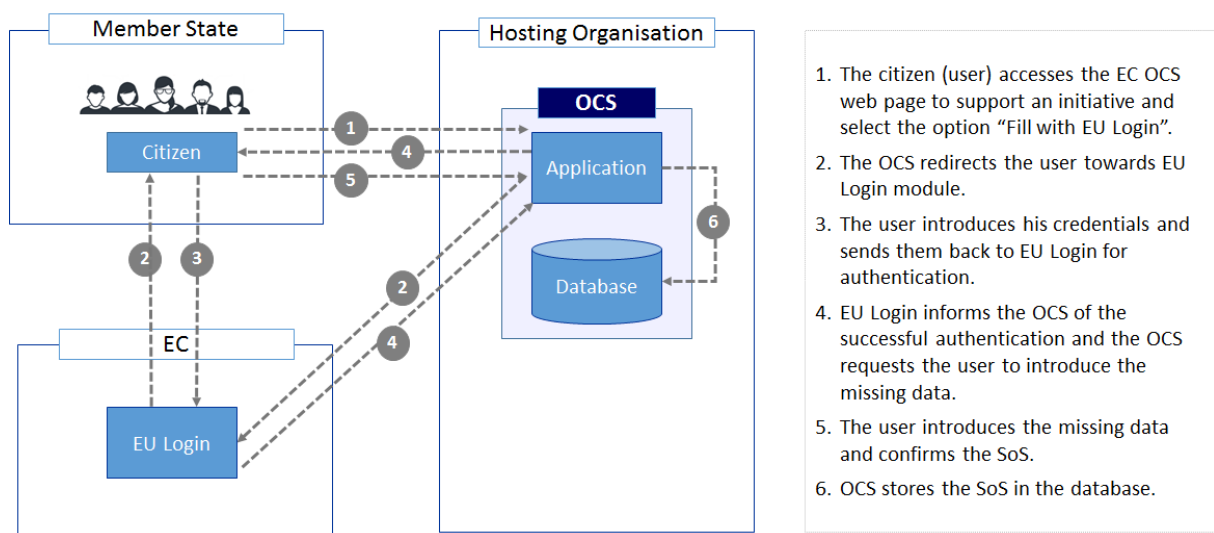


Figure 22: Architecture and dataflows for EU Login

A detailed description of the elements and their interaction is presented in section 17.1. The OCS is updated to support the changed navigation, as well as with the inclusion of the EU Login connection module.

Changes in the navigation in the OCS

The navigation in the OCS will need some changes, such as the inclusion of a button to connect to the EU Login system and receiving the response. These are considered minor changes.

Inclusion of the modules to connect to the EU Login system

The EU Login module sends an authentication request through the user's browser to the EU Login system, where the user authenticates via his/her EU Login account. When this module receives a response from the EU Login system, the certificate used for signing is extracted and compared with the stored certificate of the EU Login system. Thanks to this comparison, the sender of the response message is verified.

The documentation for the connection, as well as the corresponding software modules are available at DIGIT. The database does not require any change as the inclusion of the source of the data in the database is not considered as a trustworthy contribution to the collection process.

The user's PC or mobile device needs to support Web navigation. This software is usually installed by default and is already needed in the current version of the OCS. Also the EU Login system will remain unaltered.

Use Case 2: Verification of statements of support

The business process *verification of statements of support* is the same as this process described in 4.1.2, replacing the signed PDF documents with traditional electronic statements of support.

8.2 DATA PRIVACY OVERVIEW

The main legal concern that could be raised regarding a possible connection between the OCS and EU Login is regarding privacy of the data stored in EU Login accounts. According to EU Login's privacy statement, only personal information entered manually by the user or provided by the public organisation him/her belongs to when granting access to the system is stored. By opening the account, the user authorises the disclosure to any Commission site that is accessed via EU Login

Regarding the use of such data, the EC will not divulge the information with two exceptions:

- The duly authorised support unit or help desk.
- Duly authorised bodies, on a case by case basis (e.g. Internal Commission Security Directorate)

Passwords are encrypted and stored only in a reversible form. In addition, the details about user accounts (date and time of authentication, password changes etc.) are available only to the user and the service administrators.

In light of the information presented, EU Login presents security features that make it a suitable solution for a potential integration with the OCS.

8.3 BUSINESS ANALYSIS

The complementing solutions aim at providing additional features to the OCS, supporting the online submission of statements of support. Solution 5 foresees the possibility of linking both the EU Login (formerly ECAS) to the ECI entry point. Users would authenticate themselves and the data stored in their accounts would be used for pre-filling the data fields required to submit a statement of support.

From a usability point of view, the EU Login solution only has a minor impact on the ECI website. A button for the use of EU Login is added on the page where the user has to enter his/her data. The use case described in the functional view (see section 8.1.2) details all the steps required to complete the process.

The data stored in external EU Login accounts is very limited. Therefore, although the signatory will find a user-friendly procedure, the time devoted to complete the submission of the statement of support will increase as he/she introduces the remaining data. Currently, external accounts only store the full name of the user and his/her email. Internal accounts (owned by people professionally involved with the European Commission) store additional information relevant to the ECI requirements, such as date of birth, place of birth and nationality. Consequently, regular citizens who hold a valid external EU Login account have to input manually the rest of the personal data requirements.

Given the fact that the creation of EU Login as an integrating access point for all the EU services is relatively new, it is not yet used by a significant percentage of the EU population. Besides, only internal accounts have a substantial amount of data to be retrieved when supporting an initiative. The number of accounts validated can be considered as minimal, as it is mainly restricted to EU officials and other internal workers.

Therefore, the penetration of this complementary solution is not expected to be high, as the EU Login account is still in an early stage of growth.

The following table provides a summarised version of the assessment of this solution regarding the selected evaluation criteria:

Evaluation Criteria	Score	Description
Ease of use	● ● ○ ○ ○	<ul style="list-style-type: none"> The user will have to give his/her consent for the retrieval of data. In a few clicks, and after entering his username/password (and possibly go through the two-step authentication) the data will be pre-filled in the OCS. The user would not be required to complete the captcha before submitting the statement of support
Quantity of data	● ○ ○ ○ ○	<ul style="list-style-type: none"> EU Login external accounts currently store very little information about citizens. Therefore, the user will still need to enter most to the data fields manually
Penetration	● ○ ○ ○ ○	<ul style="list-style-type: none"> EU Login is a fairly new service that is not currently used by a significant part of the EU population

Figure 23: Summary of the business analysis – EU Login

8.4 TECHNICAL ANALYSIS

The main benefit of this solution is the scalability and maintainability: new eIDs can be integrated without any effort, and changes in the existing eIDs are transparent for this solution. Also the ease of integration should be highlighted, and as a consequence the expected little cost/efforts. However, no

significant increase of the security can be expected, as the user's data as just as reliable as in the current implementation of the OCS.

The above-mentioned information is summarised in the following table:

Evaluation Criteria	Score	Description
Scalability	● ● ● ● ●	There are no scalability issues for this solution. New eIDs or new Member States are irrelevant for this solution.
Maintainability	● ● ● ● ●	No maintainability issues are expected.
Performance & usage of resources	● ● ● ● ○	The CPU usage will increase in an important percentage (around 70%), but the throughput of a modern server is sufficient to support many initiatives in parallel. Performance tests in the STORK project have shown that a modern server can produce and verify some 50 signatures per second, which is 4M signatures per day.
Security on data storage	● ● ● ○ ○	No changes are expected.
Fraud prevention	● ● ● ○ ○	No changes are expected.
Security on data transmissions	● ● ● ○ ○	No changes are expected.
Session management	● ● ● ○ ○	No changes are expected.
Ease of integration	● ● ● ● ●	This solution is easy to integrate. Just one module with a simple API is to be integrated. Examples for integration are available.
Maturity	● ● ● ● ●	All the underlying technologies exist on the market since several years.
Portability	● ● ● ● ●	The solution with Java is portable with little effort.
Cost/Efforts	● ● ● ● ●	This solution can be implemented with a low cost. Estimations are around 3 man-months

Table 25: Summary of the technical analysis – EU Login

8.5 ASSESSMENT

Solution 5 might be introduced as complement to the current procedure to submit statements of support through the OCS. The user would be able to connect to EU Login in order to retrieve the relevant data stored in those accounts, which will pre-fill the data fields required by the corresponding Member States. The user interface would then be modified, including specific buttons that allow for a connection with both platforms.

Regarding EU Login, the following diagram presents a summary of the evaluation carried out, focusing on business and technical criteria. Detailed information about the assessment evaluation criteria can be found in Appendix F – Solution 5: Prefilling user's data with EU Login.

Solution 5- Pre-filling with EU Login

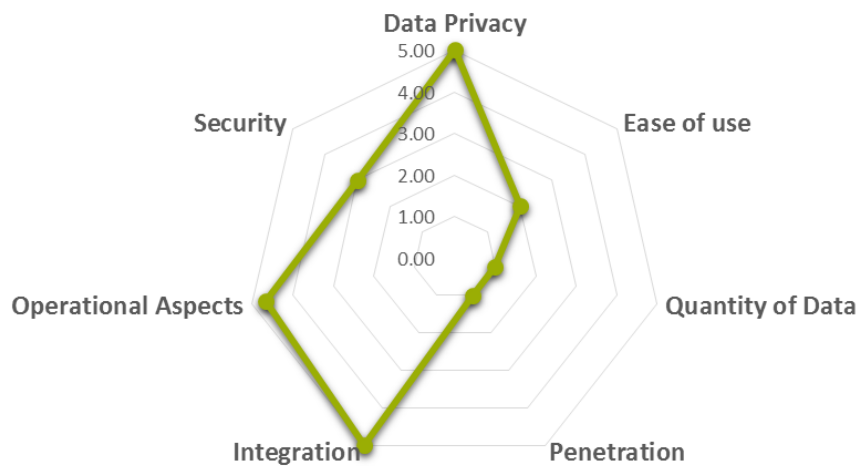


Figure 24: Assessment of solution 5 – EU Login

As can be seen in the graph, setting aside the current limitation due to the absence of dedicated eIDAS node at EU level, this solution obtains high scores regarding its implementation and maintenance, given the fact that no interaction with Member State will take place and the retrieval of the information can be achieved at a relatively little effort and cause, providing the added value of the two-step authentication, an enhance security feature to bypass the CAPTCHA.

On the other hand, and given the absence of relevant information in the external EU Login accounts, the user will need to pre-fill the data requirements manually, as only the full name could be retrieved, causing the low scores assigned to the Ease of use and Quantity of data criteria. Moreover, EU Login is a relatively new platform, and therefore not much known across the EU. However, as it inherits the ECAS database, all these old accounts have been integrated into it. Anyway, the ECAS accounts cover people with regular contacts with the EC, which is around 1% of the EU population.

9 SOLUTION 6: PREFILLING USER'S DATA WITH FACEBOOK

9.1 DESCRIPTION

9.1.1 Introduction

This chapter analyses two complementing tools for prefilling a statement of support: Facebook. This solution can be used to retrieve data from the user's account, easing the process of supporting an ECI by reducing the amount of data to be filled manually by the user and possibly by removing the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).

As Facebook does not perform any check on authenticity of the data introduced by the user, there is no way to certify the accuracy of these data, and the prefilled fields of the statement of support should remain editable. This way, the user can still bring modifications and adapt some data if necessary. The user then fills in the data not present in the EU Login account manually.

Besides EU Login and social network integration, a third method of pre-filling exists: most browsers allow pre-filling previously typed contents, although their implementations are slightly different:

- Firefox remembers contents typed on the previously visited forms; when visiting the same form again and typing the first character it automatically displays a list of previously typed contents for the field; and so on for each field on the form.
- Chrome allows remembering the contents typed on the previously visited form, it asks whether or not to remember these contents; when visiting the same form again, and it automatically fills all fields with the previously typed contents.
- Edge must be configured in order to remember the contents of previously typed contents.

This pre-filling, also called auto-completion improves the user experience, but has no effects on the OCS. Consequently, this feature is not further studied in this document.

9.1.2 Functional view

Use Case 1: Collection of statements of support

The architecture and dataflows of this solution are presented in the following diagram.

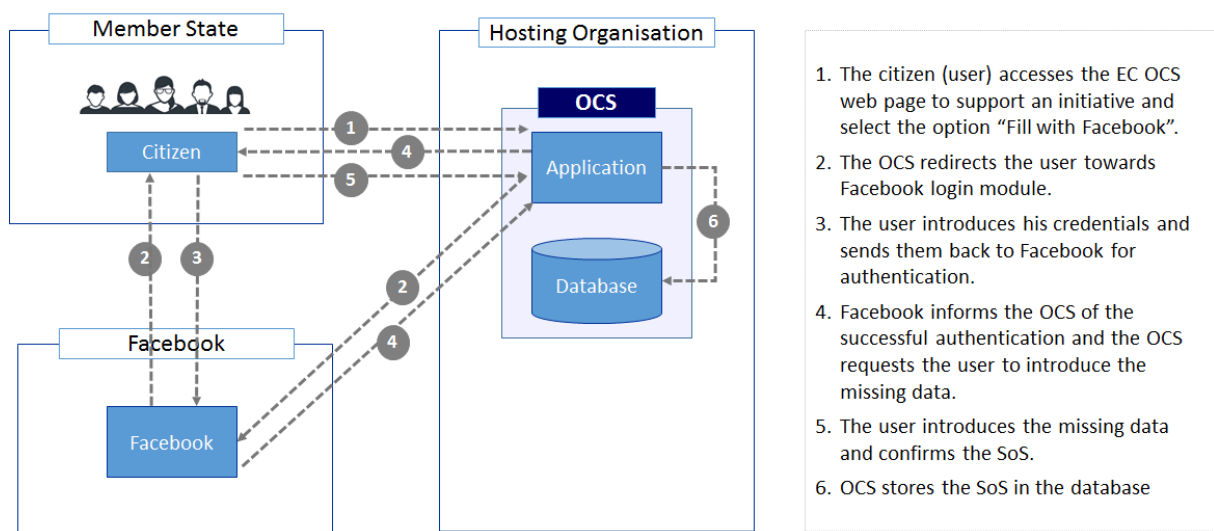


Figure 25: Architecture and dataflows for Facebook

A detailed description of the elements and their interaction is presented in section 18.1.1.

Use Case 2: Verification of statements of support

The business process *verification of statements of support* is the same as this process described in 4.1.2, replacing the signed PDF documents with traditional electronic statements of support.

9.2 DATA PRIVACY OVERVIEW

The main legal issue to be assessed when attempting to establish a connection between the OCS and EU Facebook is regarding privacy of the data stored in Facebook accounts, and the information that Facebook might store when a user accesses a Facebook service (like and share buttons, Log in, session tracking, etc.).

According to Facebook's privacy agreement, by opening the account, the user authorises Facebook to store such data. Nevertheless, the user can choose which personal information he is willing to disclose and to modify such parameters at any moment of time.

In case Facebook services are incorporated into the OCS, when any user accesses them (log in with Facebook, or share the content of an initiative) Facebook also stores information regarding the use of such services, and the website or application that uses those services. Facebook can, in virtue of agreements subscribe with them, share that information with vendors, services providers and other partners who support their business. It is inferred that such agreements are based on confidentiality obligations that both parties oblige to.

Moreover, in its data policy, Facebook states that the information collected within the European Economic Area ("EEA") may be transferred to countries outside of the EEA. However, it utilises standard contract clauses approved by the European Commission and obtain the user's consent to legitimise data transfers from the EEA to the United States and other countries³³.

This may pose a concern regarding what specific information would Facebook have access to, and where this would be stored, regarding citizens and also organisers of any given initiative.

9.3 BUSINESS ANALYSIS

With, more than 1.86 billion users worldwide³⁴, Facebook is one of the most widely used social networks. It had 247,070,000 users in the EU in June 2016, and is used by a wide variety of citizens from all ages.

The process for retrieving the data is very simple, as the user only has to authorise the retrieval of information from his/her Facebook profile. Once this step is completed, the data fields will be prefilled with the information stored in the Facebook account. The user will have to complete and correct this information in order to comply with the data requirements established by each Member State.

Since the user interface is not impacted by important modifications (only a button to connect with Facebook will be added), and the data will be easily retrieved, this solution will certainly reduce the complexity of the current procedure and the time devoted to finalise it.

³³ <https://www.facebook.com/policy.php>

³⁴ <http://www.internetworldstats.com/stats9.htm>

As of today, Facebook users can store the following personal data fields relevant for the ECI requirements:

- Name
- Surname
- Date of birth
- Address

Taking into consideration these pieces of data and putting them in contrast with the different personal data currently required by each Member States (as stated in Annex III of the Regulation), the results are diverse, depending on the Member State. The following table shows a comparison between the personal data requirements and the data stored in Facebook accounts.

Legend	
x	Present/Required
	Not required/not present
	EOI requirement not present in Facebook

	Name		Father's name		Name at birth		Residence		Date of birth		Place of birth		Nationality		Personal Identification Number	
	EOI Personal data requirements	Facebook	EOI Personal data requirements	Facebook	EOI Personal data requirements	Facebook	EOI Personal data requirements	Facebook	EOI Personal data requirements	Facebook	EOI Personal data requirements	Facebook	EOI Personal data requirements	Facebook	EOI Personal data requirements	Facebook
Austria	x	x					with full address details	x	x	x	x		x		x	
Belgium	x	x					x	x	x	x	x		x			
Bulgaria	x	x	x					x		x			x		x	
Croatia	x	x					with full address details	x		x			x		x	
Cyprus	x	x						x		x			x		x	
Czech Republic	x	x						x		x			x		x	
Denmark	x	x					x	x	x	x	x		x			
Estonia	x	x					x	x	x	x	x		x			
Finland	x	x					Only the country	x	x	x			x			
France	x	x					with full address details	x	x	x	x		x		x	
Germany	x	x					x	x	x	x	x		x			
Greece	x	x	x		x			x	x	x			x		x	
Hungary	x	x						x		x			x		x	
Ireland	x	x					x	x	x	x			x			
Italy	x	x					with full address details	x	x	x	x		x		with issuing authority	
Latvia	x	x			x			x	x	x	x		x		x	
Lithuania	x	x						x		x			x		x	
Luxembourg	x	x					with full address details	x	x	x	x		x			
Malta	x	x						x	x	x			x		x	
Netherlands	x	x			x		x	x	x	x	x		x			
Poland	x	x					with full address details	x		x			x		x	
Portugal	x	x						x	x	x			x		x	
Romania	x	x					with full address details	x	x	x			x		x	
Slovakia	x	x			x		x	x	x	x	x		x			
Slovenia	x	x						x	x	x	x		x		x	
Spain	x	x						x	x	x			x		x	
Sweden	x	x						x		x			x		x	
UK	x	x					x	x	x	x			x			

Table 26: Comparison of the personal data requirements and the data stored in Facebook

This comparison table shows that, for some countries, the amount of data to be added is minimal whereas for others that quantity is higher.

For instance, citizens from Finland will only need to type in their nationality, as the rest of the data required by those countries could be retrieved from the signatory's Facebook account. However, citizens from countries that require additional data such as Identification number (Austria, France, Spain, Sweden, etc.), place or birth (e.g. Belgium, Denmark, Estonia or Slovakia), name at birth (Latvia, the Netherlands and Slovenia) or father's name (Bulgaria and Greece) have to provide additional of data in order to complete the submission.

When analysing the data that will be covered by the information stored in Facebook profiles, it is important to note that all the data stored in Facebook is optional. As a result, the data to be inserted will ultimately depend on what amount of data each citizen has stored in his/her Facebook account. In cases the information is not accurate, the user has to correct the fields not properly filled, increasing the final amount of data to be inserted.

When analysing the Facebook complement for the OCS, the penetration rate seems more promising. According to Eurostat, 52% of the EU population aged from 16 to 74 was engaged in the use of social networks in 2016³⁵. Specifically, Facebook has penetration rate of 39.5%³⁶ in Europe, meaning that over 307 million people have a Facebook account³⁷. Therefore, implementing a solution that links Facebook, as the main representative of social networks, to the OCS has a significant effect on penetration and will become an excellent tool to campaign for an initiative and raise awareness of the ECI tool in general.

In light of the information presented, an overview of the assessment carried out regarding this solution is presented below:




Evaluation Criteria	Score	Description
Ease of use		<ul style="list-style-type: none"> Once the user authorised the retrieving of his personal information from his Facebook account, the statement of support is automatically prefilled. Then, the user just need to correct and complete the missing data to comply with the data requirements of each Member State.
Quantity of data		<ul style="list-style-type: none"> The quantity of data to be input by the user depends on each Member State requirements. The relevant data available on Facebook are: Name, Surname, Date of birth and Address.
Penetration		<ul style="list-style-type: none"> Facebook has a penetration rate of 39.5% in Europe, meaning that over 307 million people have a Facebook account

Table 27: Summary of the business analysis – Facebook

³⁵ <http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00127&plugin=1>

³⁶ <http://www.internetworldstats.com/facebook.htm>

³⁷ <https://zephoria.com/top-15-valuable-facebook-statistics/>

9.4 TECHNICAL ANALYSIS

The main benefit of this solution is the scalability and maintainability: new eIDs can be integrated without any effort, and changes in the existing eIDs are transparent for this solution. Also the ease of integration should be highlighted, and as a consequence the expected little cost/efforts. However, no significant increase of the security can be expected, as the user's data as just as reliable as in the current implementation of the OCS.

The above-mentioned information is summarised in the following table:

Evaluation Criteria	Score	Description
Scalability	● ● ● ● ●	There are no scalability issues for this solution. New eIDs or new Member States are irrelevant for this solution.
Maintainability	● ● ● ● ●	No maintainability issues are expected.
Performance & usage of resources	● ● ● ● ○	The CPU usage will increase in an important percentage (around 70%), but the throughput of a modern server is sufficient to support many initiatives in parallel. Performance tests in the STORK project have shown that a modern server can produce and verify some 50 signatures per second, which is 4M signatures per day.
Security on data storage	● ● ● ○ ○	No changes are expected.
Fraud prevention	● ● ● ○ ○	No changes are expected.
Security on data transmissions	● ● ● ○ ○	No changes are expected.
Session management	● ● ● ○ ○	No changes are expected.
Ease of integration	● ● ● ● ●	This solution is easy to integrate. Just one module with a simple API is to be integrated. Examples for integration are available.
Maturity	● ● ● ● ●	All the underlying technologies exist on the market since several years.
Portability	● ● ● ● ●	The solution with Java is portable with little effort. Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different appservers.
Cost/Efforts	● ● ● ● ●	This solution can be implemented with a low cost. Estimations are around 3 man-months

Table 28: Summary of the technical analysis – Facebook

9.5 ASSESSMENT

This complementing solution presents similar results in relation to its ease of implementation and maintenance as the EU Login solution, although the opportunities it presents regarding the ease of use and penetration are to be taken into account, shaping the diagram in a different way:

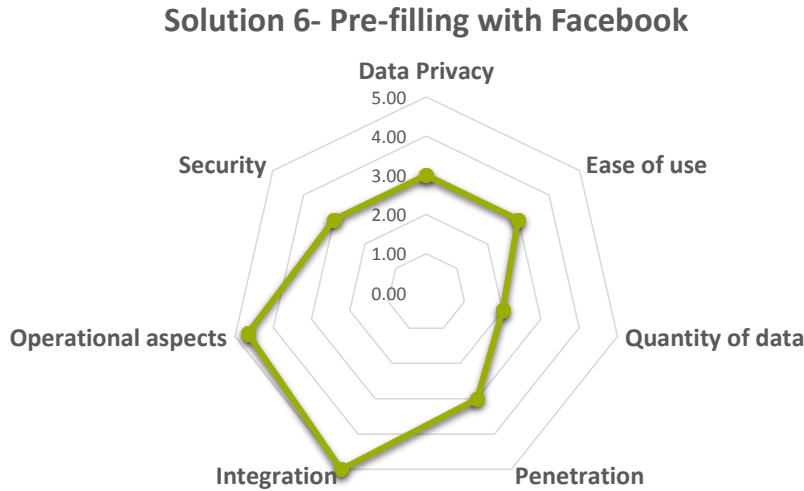


Figure 26: Assessment of solution 6 – Facebook

As mentioned, Facebook's outstanding level of penetration provides exceptional opportunities for users and organisers to raise awareness towards any initiative and the ECI tool in general. Consequently, this solution is assigned higher marks in the ease of use and especially, penetration. The data stored in Facebook provides a better score than EU Login in this criterion, although this improvement is not significant.

Similarly to EU Login, Facebook does not present significant hurdles to be implemented from a technical point of view. As a consequence, high scores are assigned to the Integration and Operational criteria.

9.6 COMPARISON OF SOLUTIONS 5 AND 6

Solutions 5 and 6 might be introduced as complements to the current procedure to submit statements of support through the OCS. The user would be able to connect to both EU Login and Facebook in order to retrieve the relevant data stored in those accounts, which will pre-fill the data fields required by the corresponding Member States. The user interface would then be modified, including specific buttons that allow for a connection with both platforms.

The following table shows the SWOT analysis for solutions 5 and 6. Despite a different penetration level, the characteristics of those two solutions are mainly similar.

	Solution 5: pre-filling data EU Login	Solution 6: pre-filling data with Facebook
Strengths	<ul style="list-style-type: none"> • Ease of use: user friendly and simplified process • Penetration: EU Login is not currently used by a significant part of the EU population 	<ul style="list-style-type: none"> • Ease of use: user friendly and simplified process • Penetration: Facebook is widely used
Weaknesses	<ul style="list-style-type: none"> • Quantity/Accuracy of data: The data present in the EU Login is not sufficient to fulfill the personal data requirements. 	<ul style="list-style-type: none"> • Quantity/Accuracy of data: The data present in the Facebook accounts is not sufficient to fulfill the personal data requirements. Besides, the information might not always be accurate.
Opportunities	<ul style="list-style-type: none"> • Two-step authentication: Enhanced security and possibility to remove the Captcha from the OCS webpage. • Awareness and publicity of ECI through social media. 	<ul style="list-style-type: none"> • Two-step authentication: Enhanced security and possibility to remove the Captcha from the OCS webpage. • Awareness and publicity of ECI through social media.
Threats	<ul style="list-style-type: none"> • n/a 	<ul style="list-style-type: none"> • Data Privacy concern: what specific information Facebook would have access to, and where it would be stored, regarding citizens and organisers of any given initiative.

Figure 27: SWOT analysis of solutions 5 and 6

As those two solutions can be easily compared from several points of view, the table hereunder provides a comparison based on a set of the identified evaluation criteria.

Evaluation Criteria	Solution 5	Solution 6	
Data Privacy	●●●●●	●●○○○	EU Login presents security features that make it a suitable solution for a potential integration with the OCS. On the contrary, regarding Facebook’s privacy agreement, there is a concern regarding what specific information would Facebook have access to, and where this would be stored, regarding citizens and also organisers of any given initiative
Member States' responses	n/a	n/a	n/a
Ease of use	●●○○○	●●●○○	For both solutions, once the user authorises his/her data to be retrieved, the statement of support is automatically prefilled. There is a possibility to remove the CAPTCHA before submitting the statement of support.
Quantity of data	●○○○○	●●○○○	With EU Login external accounts, the user still need to enter most of the data manually. With Facebook, the quantity of data to be input by the user depends on each Member State’s requirements.
Penetration	●○○○○	●●●○○	While EU Login is a fairly new service that is not currently used by a significant part of the EU population, Facebook has a penetration rate of 39.5% in Europe
Operational aspects			The operational aspects are similar for both solutions
Security	●●●●●	●●●●●	Both solutions presents similar score regarding security.
Integration	●●●○○	●●●○○	Both solution are easy to integrate, mature, portable and don’t require a lot of effort or cost to be implemented.

Table 29: Comparison of solutions 5 and 6

10 CONCLUSIONS

The objective of this study has been to further assess the potential use of eID in the context of ECI. This study has concentrated on the potential benefits of the eID integration in the process of collection and verification of statements of support in the ECI process.

As this study shows, there are a large number of complex issues to consider for technical possibilities of eID in the process of the ECI. everis approach covered the analysis of all three - legal, business and technical - requirements of each identified solution: eSigned PDF, e-signature, direct eID integration, and integration with eIDAS Framework. The complementary solutions – using EU Login or Facebook account for prefilling the statement of support in order to facilitate and to simplify the ECI process for collection and verification – were also analysed according to legal, business and technical criteria identified in chapter 2: Approach and methodology.

During the process of the study, various criteria have indeed been identified and analysed. The most important and relevant ones have been selected and formed the core of the evaluation matrix criteria, which have been applied to assess each solution and to quantify the effects of each criterion on the solution. The analysis of the strengths, weaknesses, opportunities and threats complemented each solution's assessment. For the final evaluation and comparison between the solutions, the evaluation matrix have been applied (see Appendix H – Evaluation Matrix).

From a legal point of view, several changes, both to the ECI Regulation and Implementing Regulation, are necessary for the implementation of the different solutions. Those changes are identified and summarised in the following table. More information can be found in the legal analysis of the respective solutions.

Solution	Change Required		Description
	ECI Regulation	Implementing Regulation	
1	(Yes)	Yes	Annex III Re-wording of Article 5.2 is advisable but not mandatory
2	Yes	Yes	Article 8 and Annex III Re-wording of Article 5.2 is advisable but not mandatory
3	Yes	Yes	Articles 5 & 8 and Annex III
4	Yes	Yes	Articles 5 & 8 and Annex III
5	No	No	n/a
6	No	No	n/a

Table 30: Summary of the changes required to ECI and Implementing Regulation

From overall analysis, everis has concluded that none of the analysed solutions could fully satisfy the requirements of ECI and the goal to improve and facilitate the collection and verification of signatures for statements of support, while at the same time complying with identified legal, business and technical ideal criteria in this particular context.

However, everis identified the two most promising and feasible solutions for the purpose of making an improvement in the collection of statements of support and in the verification phase of the ECI

process. Both of them have their pros and cons, and cannot be seen at the current stage of the project useful or possible to be implemented and working.

The most recommended solution for eID integration with a strong perspective to the future is the solution 4: integration with the eIDAS framework. The eID integration with the eIDAS network provides all the benefits of using the eID to sign a statement of support - from clear user's commitment to improved data quality for the campaign organizers, and from validity of the user to the simplification of the verification process of statements of support.

Furthermore, the integration with eIDAS would be also one of the most recommended options from a feasibility point of view. For this solution, the eIDAS node would be the one granting the safe access to the Member States' eID access points. Thus, there would be a need to integrate the ECI online collection system only with one node. In this way, solution 4 would be the best also from costs, maintainability and scalability point of view.

Process-wise, the user would feel no difference between the integration with the eIDAS network and the implementation of the direct eID integration (solution 3). However, from a legal point of view, solution 4 would require a specific reference to the use of eID and to the eIDAS network. In addition, it would also require Member States to discuss and agree on the level of data requirements for signing a statement of support with using eID and eIDAS. For successful implementation of the solution, the agreement on necessary data, the identification of the user and assurance of the user's eligibility criteria to sign a statement of support are equally important. Furthermore, it will be also necessary to obtain the agreement from the eIDAS expert group to use one of the eIDAS custom field to store the nationality of the signatory as this information is required for the validation of the business rules.

Another solution that was considered is the electronically signed PDF (solution 1). It has various advantages, from easy, immediate implementation to the compliance to the legal background laid in the ECI regulation. The major added value of this solution is its data security and specific association of e-signature with a specific initiative, preventing any fraud cases in reusing the provided data for any other initiative.

However, its major drawback – lower user-friendliness than any other solutions – might prevent its wider application in the ECI. There is a probability that signing a PDF would look complicated for an average user of the platform. Furthermore, the analysed solution does not simplify the verification process either, as automatic validation is not foreseen at the moment.

In brief, currently both the electronically signed PDF and the integration with the eIDAS network solutions do not provide the ideal path to simplification or facilitation of collection and verification of statements of support, but they are the ones offering the better prospects. On one hand, with future advancement of eIDAS integration, solution 4 has better prospects as the long-term solution. On the other hand, the eSigned PDF provides a short-term solution to improve the security and quality of data at a low integration cost, and if combined with one of the prefilling solutions, as analysed in this study, it could help to achieve higher user satisfaction.

Regarding the other solutions that were analysed, direct integration of eID (solution 3) and e-signature (solution 2) do not differ much in respect to legal and business requirements. As it can be

seen from their respective SWOT analysis and radar chart diagrams, both solutions are complying quite well with legal and business criteria. Proportionally, both solutions lack suitability from the technical point of view. Security, integration and operational aspects are the core drawbacks. In addition, direct eID integration bears significant implementation costs not only from the OCS side, but especially from Member States' point of view.

The complementary solutions as pre-filling option analysed in the study could be the first easiest and cheapest advancement towards facilitation of the process of statements of support collection. EU Login might not receive a substantial interest from the users' point of view, but Facebook with its high level of penetration could turn as a useful tool to simplify the process of data input for signing the statement of support. Moreover, the pre-filling options could ease the process of supporting an ECI by possibly removing the CAPTCHA. Further analysis of this functionality is being performed as part of the study on the improvement of the ECI Implementation Regulation.

To conclude, eidentification integration in the ECI cannot provide mature and fully suitable solutions for the simplification or facilitation of collection and verification of statements of support. Nevertheless, some solutions' suitability depends also on various processes, such as the advancement with the eIDAS network or the change of legislation on both the EU and Member State' level, which would strongly affect the preference for one solution over the other.

11 REFERENCES

- Anglmayer, Irmgard. (2015) *The European Citizen's Initiative: the experience of the first three years*. European Parliamentary Research Service.
[http://www.europarl.europa.eu/thinktank/es/document.html?reference=EPRS_IDA\(2015\)536343](http://www.europarl.europa.eu/thinktank/es/document.html?reference=EPRS_IDA(2015)536343)
- Bender, Jens (2015) *eIDAS Regulation: eID-Opportunities and Risks*. Fraunhofer-Gesellschaft, session V: Standardisierung. p.156-166;
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Bender.pdf?__blob=publicationFile
- Berg, Carsten & Thomson, Janice (eds.) (2014) *An ECI that Works! Learning from the first two years of the European Citizen's Initiative*. <http://ecithatworks.org/>

<https://developers.facebook.com/docs/facebook-login/web>

<https://developers.facebook.com/docs/facebook-login>

<https://ec.europa.eu/digital-single-market/en/e-identification>
- Effler, Michael (2003). *How the European Citizen's Initiative came to existence*. European Citizens' Initiative News Section. <http://www.citizens-initiative.eu/how-the-convention-got-convinced/>
Consulted on 1/12/2016
- European Commission (2016) *Areas of improvement in the functioning of the ECI. Summary of the replies received from the Member States*, Experts Group on the European Citizen's Initiative.
<http://ec.europa.eu/citizens-initiative/files/summary-report-january-2016.pdf>
- European Commission (2016) *Proposals from Austria, Germany and Luxembourg to improve the ECI*. Experts Group on the European Initiative. <http://ec.europa.eu/citizens-initiative/files/ECI-expert-group-meeting-19-01-2016-Proposals-for-ECI-improvements.pdf>
- European Commission (2015) *Report on the application of Regulation (EU) No. 211/2011 on the citizen's initiative*. Report from the Commission to the European Parliament and the Council.
<http://ec.europa.eu/citizens-initiative/public/legislative-framework?lg=en>
- European Commission (2015) *Assessment of ICT impacts of the Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative*.
- European Commission, *report from the European Commission to the European Parliament and the Council, Report on the application of Regulation (EU) No 211/2011 on the citizens' initiative*, COM(2015) 145 final
- European Parliament (2016) *Potential and Challenges of E-participation in the European Union*. Directorate-General for Internal Policies, Policy Department. Citizen's Rights and Constitutional

Affairs.

[http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU\(2016\)556949](http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2016)556949)

European Parliament (2016) *The Legal and Political Context for Setting Up a European Identity Document*. Directorate-General for Internal Policies, Policy Department. Citizen's Rights and Constitutional Affairs;

[http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU\(2016\)556957](http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2016)556957)

<https://www.facebook.com/policy.php>

Le Gouvernement du Grand-Duché de Luxembourg (2015) *Potential Benefits of Electronic Signatures in The Context of European Citizen Initiatives*.

OAuth 2.0 protocol: <https://oauth.net/2/>

Opinion of the European Data Protection Supervisor (2010). Official Journal of the European Union Volume 53. C323 ISSN 1725-2423; <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=OJ%3AC%3A2010%3A323%3ATOC>

Průša, Jiří (2015). *E-identity: Basic building block of e-Government*. In *IST-Africa Conference, 2015. IEEE*; https://www.nic.cz/files/nic/doc/Jiri_Prusa_mojID_ISTAfrica.pdf

Project: Secure idenTity acrOss boRders linKed 2.0 (STORK 2.0) (2015) *Deliverable: Stork 2.0 Member State's eIDs (January 2015)*; https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=52:stork-20-member-states-eids-january-2015&Itemid=180

RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: <https://www.ietf.org/rfc/rfc5280.txt>

Regulation (EU) 910/2014 (eIDAS Regulation): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

Treaty on European Union (Consolidated Version), Treaty of Maastricht, 7 February 1992, Official Journal of the European Communities C 325/5; 24 December 2002

12 APPENDIX A – OVERVIEW OF THE NATIONAL EID SCHEMES

	eID schemes	LoA
Austria	Austria has deployed a system based on multiple different cards that provide access to services. The Bürgerkarte “e-card”, a health insurance card, is complemented by student service cards and profession cards (public officials, lawyers, notaries, pharmacists, etc.). At the same time, the Handy-Signature, a mobile eID alternative, and the most popular eID with around 750.000 active users by 2017, is also available. This scheme uses a certificate stored in a cryptographic device, to which access is granted to the subscriber of the certificate thanks to his/her username and password combination. An extract of the resulting signature is then sent to the citizen’s mobile phone. After his/her confirmation, the signature is sent to the requesting application.	High
Belgium	Belgium’s national eID scheme is based on the public national ID card, BELPIC. Nationals from other countries residing in Belgium also have access to a foreigner's ID with the same high Level of Assurance. The card contains three private 1024-bit RSA keys, one of the keys is card-specific and the two others are citizen-specific. The card-specific key (the so-called basic private key) is used to perform a mutual authentication between the ID card and the National Register. This is required, for instance, to update the data on the card. The corresponding public key is only available to the National Register, therefore being the only authority able to verify signatures created by this private key. The first citizen-specific key is used for signing electronic documents. This key is linked to a qualified certificate allowing the identification of the citizen. The second citizen-specific key is used for authentication in eBusiness and eGovernment applications and is linked to a non-qualified certificate. The storage of data extracted from the eID in a database must be approved by the Belgian privacy commission.	High
Bulgaria	To be completed with the information provided by the MS	To be completed
Croatia	To be completed with the information provided by the MS	To be completed
Cyprus	To be completed with the information provided by the MS	To be completed
Czech Republic	The Czech national identity card is mandatory for permanent resident of 15 years old and older. Czech Republic has implemented a system, MojeID, which is based on online certificates provided by Czech accredited certification authorities, with a validity of 1 year.	Low or substantial
Denmark	To be completed with the information provided by the MS	To be completed
Estonia	Besides the national ID card, another card is also available: the Digit-ID, giving access to public services online. Estonia was also one of the first countries to introduce a mobile eID scheme that is now fully operational. This scheme uses a certificate stored in a cryptographic device, to which access is granted to the subscriber of the certificate thanks to his/her	High

	username and password combination. An extract of the resulting signature is then sent to the citizen's mobile phone. After his/her confirmation, the signature is sent to the requesting application.	
Finland	The Finnish Electronic Identity (FINEID) card is a non-mandatory electronic identity card that is intended to facilitate access to e-Government services for Finnish citizens and permanent residents of Finland as from 18 years. This smart card includes qualified certificates supporting authentication, encryption, and digital signature. In addition, health insurance information may be included in the ID card, replacing the KELA card.	High
France	France does not issue eID cards. However, digital certificates are available through the French Chamber of Commerce Certification Authority. The duration of the authentication and qualified electronic signature certificates stored in the tokens is 3 years.	To be completed
Germany	Germany implemented a national eID system, nPA, based on smart cards that has been working from 2010. These cards are contactless (RFID), protected against unauthorised access with the PACE protocol. Only service providers authenticated at the German Federal Office for Information Security can have access to this card. The German eHealth card (elektronische Gesundheitskarte, eGK), an insurance card for German citizens, is part of the national health telematics infrastructure. The access to this eID by service providers is not limited by the requirement of an approval of BSI as the nPA.	High
Greece	There is no official eID card in Greece. However, a Digital Signature-Authentication Card is delivered for services based on ID card information. Two other eID tokens are also available, all being valid for a period of 5 years. The electronic Identity provider "ERMIS" is connected, in preproduction, to eIDAS. TAXIS is the other widely used card, mostly used in G2G services.	ERMIS card: High TAXIS: Low
Hungary	To be completed with the information provided by the MS	To be completed
Ireland	To be completed with the information provided by the MS	To be completed
Italy	Two different eID tokens are available in Italy, the national ID card (CIE) and the national service card (CNS) issued to public servants with a validity of three years. Unlike the CIE, produced individually for every citizen, the CNS cards are mass produced and sent by mail to their card holders. At that stage, the authentication certificate is disabled. To activate it, the CNS card holder is required to go, in person, to a regional health centre, where its ID card is used to validate its identity and activate the authentication certificate.	To be completed
Latvia	To be completed with the information provided by the MS	To be completed
Lithuania	The Lithuanian eID card was first rolled out in 2009, with a total distribution of 2.49 M cards as of December 2012. The eID card features contactless technology for identity verification at border crossings, based on a fingerprint check, and embeds a contact microprocessor which contains two	ID card: substantial Civil servants eID card: High

	separate certificates for authentication and contract signing, according to the initial announcement. Both the personal identity card and the civil servants ID card can be used as eID tools in Lithuania. They are respectively granted a substantial and high Level of Assurance.	
Luxembourg	In addition to the national ID, three other tokens are available in Luxembourg: the Smart Card, the Signing Stick and the Signing Server Certificate.	High
Malta	To be completed with the information provided by the MS	To be completed
Netherlands	Two different eID tokens are available in the Netherlands: DigiD and eHerkenning. DigiD credentials are based on username/password. The certificates of eHerkenning are issued to representatives of companies, with a validity of the certificates of 3 years. The DigiD does not contain the citizen number (BSN). Consequently, it cannot be used by the private sector.	DigiD: Low, substantial eHerkenning: Substantial, high
Poland	To be completed with the information provided by the MS	To be completed
Portugal	The Portuguese Citizen Card (“Cartao de Cidadao”) is mandatory and issued to any person in the population register at the age of 6. The Portuguese Citizen Card is a physical identity document, which allows citizens to use a multichannel system in their interactions with services from the public and private sectors.	High
Romania	To be completed with the information provided by the MS	To be completed
Slovakia	The National ID card provides four different certificates: authentication certificate, QES certificate, signature certificate and encryption certificate.	High
Slovenia	In Slovenia different qualified certificates are available, but the national citizen’s card is not used as an eID token.	To be completed
Spain	Spanish national ID card is fully operational. The system is complemented by more than 27 authorised entities that issue soft certificates and certificates in crypto devices. In 2015 a new eID system called Cl@ve has been introduced. This system is based on username and password, sometimes reinforced with an SMS. The most used eID is the certificate issued by the FNMT (Royal Mint).	Certificates: substantial, high Cl@ve: low, substantial
Sweden	More than 14 different eID tokens are available, including the ID-card for the tax agency. Most of these tokens are issued by banks.	Substantial, high
UK	The gov.uk verify service is a gateway to identity services offered by specialised companies like CitizenSafe, Digidentity and Secureidentity, as well as such services offered as an additional product of other public or private entities like Barclays, Post Office and Royal Mail.	To be completed

Figure 28: Overview of the national eID schemes

13 APPENDIX B – SOLUTION 1: ELECTRONICALLY SIGNED PDF DOCUMENT

13.1 DETAILED DESCRIPTION

A European citizen supports an initiative by means of a signed PDF document. To prove the citizen's entitlement to support this initiative, he/she signs a PDF document downloaded from the OCS website, with his/her national eID enabled for signing, and uploads the signed PDF to the OCS website.

Action ID	Actor	Description
1	Citizen	The citizen decides to support an initiative. After reading the details of the initiative, he/she clicks on the button "Support", leading to the OCS.
2	OCS	The user is requested to indicate his home country, and depending on this country, he/she is requested to fill his/her personal data.
3	Citizen	The user clicks the "Download PDF" button
4	OCS	The OCS composes the PDF: it fills the user's data, as introduced, in the template PDF, and includes the name of the initiative. The composed PDF is then sent to the user.
5	Citizen	The citizen receives the PDF and opens it with the standard PDF reader. This is the PDF reader configured as standard in his PC or mobile device.
6	PDF reader	The PDF reader in the user's PC shows the contents of the received document. The document contains instructions how to produce an electronic signature
7	Citizen	Following the instructions in the document, the user requests the PDF reader to produce a signature.
8	PDF reader	The PDF reader requests the user to select a signing certificate.
9	Citizen	The citizen selects the signing certificate issued by his national eID authority. If the certificate is stored in a cryptographic device, the user will have to introduce its PIN.
10	PDF reader	The PDF reader uses the private key associated to this certificate to produce a signature. This signature, together with the used certificate is embedded in the PDF according to the PAdES standard. This signed PDF is sent to the user.
11	Citizen	When receiving this signed PDF document, the user stores it on his local disk.
12	Citizen	The citizen clicks the "Upload signed PDF" button, and selects the signed PDF to be sent to the OCS.

13	OCS	When receiving the signed PDF, the OCS extracts the certificate from it.
14	OCS	<p>The OCS validates this certificate with some basic checks. These basic checks include:</p> <ul style="list-style-type: none"> • Validity, according to the validity period: notBefore and notAfter are compared with the current system time • If the certificate is issued in a EU Member State: the “C” attribute of the issuer of the certificate is compared with the list of 28 Member States • If the issues is mentioned in the TSL of its Member State, thus the certificate is qualified • If the certificate is enabled for signing (keyUsage includes contentCommitment) • If the certificate is issued to a natural person (the OID is included in a list of OIDs of natural persons for the corresponding Member State) <p>These checks do not include the check on the status of the certificate.</p>
15	OCS	The OCS presents the statement of support with the signed PDF embedded in the page, and requests the user to confirm his support to this initiative.
16	Citizen	The citizen confirms his support to the initiative by clicking on the button “Support”.
17	OCS	The OCS stores this statement of support in its database.

Figure 29: Description of the actions for the collection of statements of support

13.1.1 Use Case 1: Collection of statements of support

The procedure to submit a statement of support making use of this solution is detailed in the following use case:

Electronically signed PDF Document. Collection phase	
Name	Creation of a statement of support signed electronically in a PDF document.
Description	The user downloads a PDF document from the ECI website, in order to apply an e-signature to support an initiative.
Actor (Generic)	EU citizen with the right to vote for the EP.
Preconditions	<ul style="list-style-type: none"> • The user has a valid e-signature certificate available • The user has a PDF reader software that allows for the use of e-signature
Basic flow	<p><u>e-signature via PDF Document</u></p> <p>The user:</p> <ol style="list-style-type: none"> 1. Accesses the ECI website

	<ol style="list-style-type: none"> 2. Selects a specific initiative to support 3. Clicks in the “Support” button 4. Selects “Download PDF document” 5. Opens the document on his local computer 6. Selects the option to use e-signature 7. Selects his certificate 8. If the certificate is stored in a cryptographic device, the user introduces his PIN 9. Saves the signed PDF document 10. In the Initiative’s website, selects the option “Upload e-signed Statement of support” 11. Selects the PDF file 12. Confirms the submission of the statement of support
Alternative flow 1	<p><u>e-signature with the user filling his/her data</u></p> <p>The user:</p> <ol style="list-style-type: none"> 1. Accesses the ECI website 2. Selects a specific initiative to support 3. Clicks in the “Support” button 4. In the data-filling webpage, selects his/her country 5. Fills the required data 6. Once his data is filled, selects “Download PDF document” 7. Opens the document in his local computer 8. Selects the option to use e-signature 9. Selects the e-signature certificate 10. If the certificate is stored in a cryptographic device, the user introduces his PIN 11. Saves the signed PDF document 12. In the Initiative’s website, selects the option “Upload eSigned Statement of support” 13. Selects the PDF file 14. Confirms the submission of the statement of support
Exception flow	<ul style="list-style-type: none"> • The certificate cannot be read by the PDF reader software • The internet browser used does not support the use of the eID certificate • The certificate is no longer valid, revoked or cannot be read • The signature received by the OCS is not qualified <p><u>Resolution</u>: statements of support can be submitted by typing data into the OCS</p>
Post conditions	<ul style="list-style-type: none"> • The statement of support of an initiative is submitted.
Devices	<ul style="list-style-type: none"> • Computer • As far as the certificate is stored in a smartcard, a card reader must be connected to the computer

Software	<ul style="list-style-type: none"> • PDF reader software that allows adding e-signature • A web browser³⁸
-----------------	--

Figure 30: Use case: electronically signed PDF document - collection phase

Depending on the possibility to accept statements of support signed under this use case, the implementation of this solution will follow different paths. The ideal scenario described in the basic flow assumes that statements of support will be submitted only with the data contained in the e-signature certificate, without requiring any additional data.

Alternatively, if e-signatures need to be complemented with additional data (see section 13.3.2), alternative flow 1 is a viable option, where users will have to enter manually the data not contained in the e-signature before downloading the PDF document.

Actors

Actor	Description
Citizen	A European citizen, with the right to vote in elections for the European Parliament, willing to support an initiative
PDF reader	A software tool designed to read documents in Portable Document Format (PDF)
OCS	A system designed to collect statements of support for initiatives

Table 31: Actors for the collection of statements of support

³⁸ The list of supported web browsers has yet to be established.

Activity diagram

The following diagram illustrates the actions and dataflows between the involved parties in the collection phase.

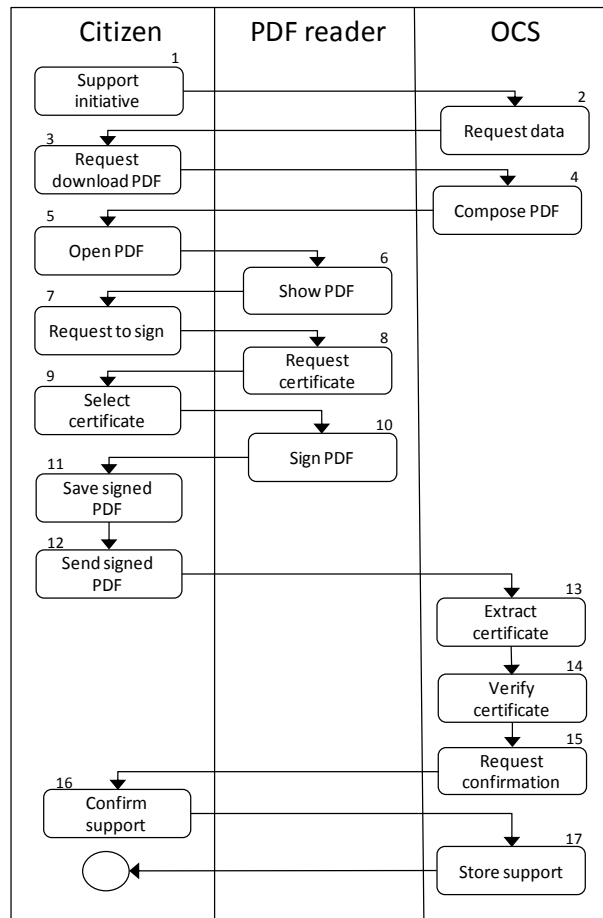


Figure 31: Activity diagram of the collection process

Action 14 is worth being highlighted: verify certificates entail that the OCS validates this certificate with some basic checks. These basic checks include:

- Validity, according to the validity period: notBefore and notAfter are compared with the current system time
- If the certificate is issued in a EU Member State: the “C” attribute of the issuer of the certificate is compared with the list of 28 Member States
- If the issuer is mentioned in the TSL of its Member State, thus the certificate is qualified
- If the certificate is enabled for signing (keyUsage includes contentCommitment)
- If the certificate is issued to a natural person (the OID is included in a list of OIDs of natural persons for the corresponding Member State)

These checks do not include the validation of the status of the certificate.

Detailed description of the activities

A European citizen supports an initiative by means of a signed PDF document. To prove his/her identity, he/she signs a PDF document downloaded from the OCS website, with his/her national eID enabled for signing, and uploads the signed PDF to the OCS website.

Action ID	Actor	Description
1	Citizen	The citizen decides to support an initiative. After reading the details of the initiative, he/she clicks on the button "Support", leading to the OCS.
2	OCS	The user is requested to indicate his home country, and depending on this country, he/she is requested to fill his/her personal data.
3	Citizen	The user clicks the "Download PDF" button
4	OCS	The OCS composes the PDF: it fills the user's data, as introduced, in the template PDF, and includes the name of the initiative. The composed PDF is then sent to the user.
5	Citizen	The citizen receives the PDF and opens it with the standard PDF reader. This is the PDF reader configured as standard in his PC or mobile device.
6	PDF reader	The PDF reader in the user's PC shows the contents of the received document. The document contains instructions how to produce an electronic signature
7	Citizen	Following the instructions in the document, the user requests the PDF reader to produce a signature.
8	PDF reader	The PDF reader requests the user to select a signing certificate.
9	Citizen	The citizen selects the signing certificate issued by his national eID authority. If the certificate is stored in a cryptographic device, the user will have to introduce its PIN.
10	PDF reader	The PDF reader uses the private key associated to this certificate to produce a signature. This signature, together with the used certificate is embedded in the PDF according to the PAdES standard. This signed PDF is sent to the user.
11	Citizen	When receiving this signed PDF document, the user stores it on his local disk.
12	Citizen	The citizen clicks the "Upload signed PDF" button, and selects the signed PDF to be sent to the OCS.
13	OCS	When receiving the signed PDF, the OCS extracts the certificate from it.
14	OCS	The OCS validates this certificate with some basic checks. These basic checks include: <ul style="list-style-type: none"> • Validity, according to the validity period: notBefore and notAfter are compared with the current system time • If the certificate is issued in a EU Member State: the "C" attribute of the issuer of the certificate is compared with the list of 28 Member States

		<ul style="list-style-type: none"> • If the issues is mentioned in the TSL of its Member State, thus the certificate is qualified • If the certificate is enabled for signing (keyUsage includes contentCommitment) • If the certificate is issued to a natural person (the OID is included in a list of OIDs of natural persons for the corresponding Member State) <p>These checks do not include the check on the status of the certificate.</p>
15	OCS	The OCS presents the statement of support with the signed PDF embedded in the page, and requests the user to confirm his support to this initiative.
16	Citizen	The citizen confirms his support to the initiative by clicking on the button "Support".
17	OCS	The OCS stores this statement of support in its database.

Figure 32: Description of the actions for the collection of statements of support

13.1.2 Use Case 2: Verification of statements of support

Once the collection phase of an initiative comes to an end and the number of statements of support gathered has reached both the total and the national thresholds, the verification phase begins and organisers must send the statements of support to the corresponding verifying authorities. The statements of support will be sent according to Article 8 of the Regulation, using the form set out in Annex V.

A variation on this process could be thought of: instead of sending the complete statements of support, only the used certificates could be sent. However, this would require a change in the Regulation. Furthermore, the difference in size between a PDF document and a certificate is around 5 KB; if compressed this difference is even far less. One more benefit of sending the signed PDF documents is that the viewer is present in most PCs, which is not the case for certificate viewers

This procedure could also be expedited by the use of e-signature, easing the identification of the representative of the organisers committee and fostering the use of an electronic format in order to complete this phase of the ECI process. The following use case depicts the process of delivering the signed statements of support to verifying authorities:

Electronically signed PDF Document. Verification phase	
Name	Submission of the collected statements of support to the corresponding verifying authorities.
Description	The user creates a PDF document in which he/she includes all the statements of support collected, and signs it electronically.
Actor (Generic)	<ul style="list-style-type: none"> • Member of the organiser's committee registered as a representative (contact person) or substitute.

Preconditions	<ul style="list-style-type: none"> • The representative has a valid e-signature certificate available • The user has a PDF reader software that allows for the use of e-signature
Basic flow	<p><u>e-signature via PDF Document</u></p> <p>The representative:</p> <ol style="list-style-type: none"> 1. Creates a document following the form of Annex V in PDF format 2. Includes the requested information regarding the initiative (title of the initiative, Commission registration number, Date of registration, etc.) 3. In the Annexes, includes all the statement of support to be verified, separating those in paper, submitted in the OCS and the eSigned PDF documents 4. In the Annexes, includes the corresponding certificates of conformity of the OCS with the Regulation 5. Selects the option to use e-signature 6. Selects his certificate 7. If the certificate is stored in a cryptographic device, the user introduces his PIN 8. Saves the PDF file
Exception flow	<ul style="list-style-type: none"> • The certificate cannot be read by the PDF reader software • The certificate is no longer valid, or revoked <p><u>Resolution</u>: the form including the statements of support collected will have to be filled by the representative including all his personal information, the date, and his/her signature.</p>
Devices	<ul style="list-style-type: none"> • Computer • As far as the certificate is stored in a smartcard, a card reader must be connected to the computer
Software	PDF reader software that allows adding e-signatures.

Figure 33: Use case: electronically signed PDF document - verification phase

As shown in the use case, the procedure for sending the statements of support for verification stated in Article 8 of the Regulation will be followed, adding the possibility to sign the form containing such important information via e-signature.

Actors

Actors	Description
Organisers	The group of people responsible for presenting the initiative and all management around it.
MS verification	The verification authority within each Member State, in charge of verifying the Statements of support for this country.
EC	European Commission
OCS	A system designed to collect statements of support for initiatives

Table 32: Actors for the verification of statements of support

Activity diagram

The following diagram illustrates the actions and dataflows between the involved parties in the verification phase.

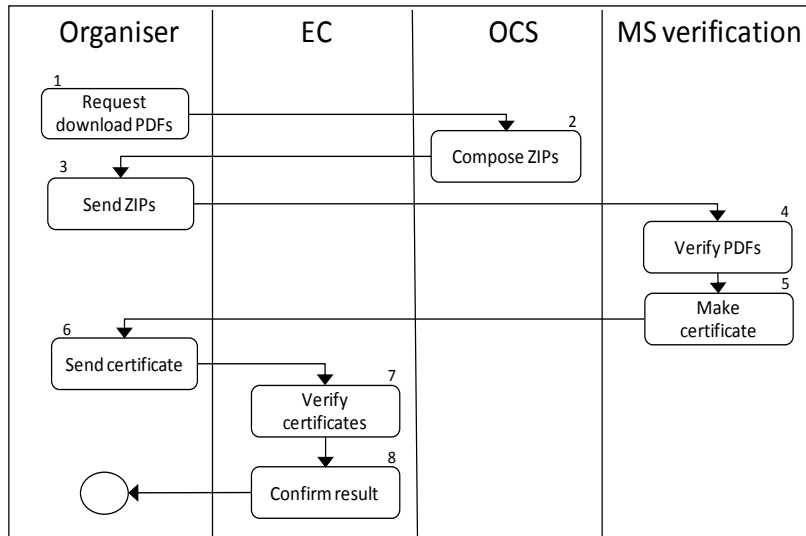


Figure 34: Activity diagram of the verification process

Detailed description of the activities

When the collection phase ends, the organisers of an ECI send the statements of support to the Member State’s verification authority, using the form set out in Annex V and separating the statements of support collected in paper form from those collected through an OCS.

Currently, the procedure for sending the statements of support to the Member States’ verification authority is not homogeneous: several methods for sending are used by different Member States. This study proposes a method to be used by all Member States.

Action ID	Actor	Description
1	Organiser	Request download PDFs The organiser requests the download of the collected statements of support with signed PDF documents.
2	OCS	Compose ZIPs The OCS encrypts the zipped file and stores it on a file server, and sends the link to this file, together with the decryption key by secure email to the organiser.
3	Organiser	Send ZIPs The organiser sends the link to this file, together with the decryption key by secure email to the corresponding Member State’s verification authority. The email message is protected for integrity by the organiser’s signature, and for confidentiality encrypted with the recipient’s public key.
4	MS verification	Verify PDFs The Member State’s verification authority views the PDFs with a

		PDF reader, and verifies the certificate used for signing was valid at the time it was used, and check if any duplicates exist with other means of supporting initiatives
5	MS verification	Make certificate With the results of the previous verification, a verification certificate is issued by the verification authority and sent to the organisers.
6	Organiser	Send certificates The organisers accumulate all verification certificates, and once all have been received, he/she sends them to the European Commission.
7	EC	Verify certificates The EC validates the received certificates, and validates that these are signed by the organisation authorised for this Member State.
8	EC	Confirm result The EC confirms the results of the initiative (the number of valid statements of support, and consequences) to the organisers

Table 33: Description of the actions for the verification of statements of support

13.2 OVERVIEW OF THE LEGAL FRAMEWORK

13.2.1 Analysis of the ECI Regulation

	Solution 1- Description	Requirements (ECI)	Review
Submission of statements of support	<p>Solution 1 is based on the use of a PDF document that the citizen downloads on his/her computer and signs using an electronic signature. This signed PDF document is then uploaded into the OCS.</p>	<ul style="list-style-type: none"> ○ Art. 5.1(ECI): only forms that comply with Annex III may be used for the collection of statements of support. ○ Art. 5.2 (ECI): statements of support may be collected in paper form or electronically. <p>Statement of support signed with advanced electronic signatures shall be treated in the same way as those submitted in paper form.</p> <ul style="list-style-type: none"> ○ Art. 6.1(ECI) the OCS shall be certified in accordance with Article 6.3 by the competent authority of the Member State in which the data will be stored. <p>The models for the statement of support forms may be adapted for the purpose of the online collection.</p> <ul style="list-style-type: none"> ○ Art. 6.2 (ECI): The OCS shall be compliant with the conditions stated in Article 6.4. ○ Art. 6.3 (ECI): the relevant authorities shall issue a certificate (according to the model set out in Annex IV) confirming the OCS complies with the requirements of Art. 6.4. ○ Art. 6.4 (ECI): Online collection systems shall have the adequate security and technical features in order to ensure that: <ul style="list-style-type: none"> ○ only natural persons may submit a statement of support; ○ the data provided online are securely collected and stored, in order to ensure, inter alia, that they may not be modified or used for any purpose other than their indicated support of the given citizens' initiative and to protect personal data against accidental or unlawful destruction or accidental loss, alteration or unauthorised disclosure or access; ○ the system can generate statements of support in a form complying with the models set out in Annex III, in order to allow for the verification by the Member States in accordance with Article 8(2). 	<p>Submission of statement of support is submission of statements of support, this solution will follow the data requirements set out in Annex III in order to generate the PDF document that will be downloaded by the user and signed using qualified e-signature, complying with Articles 5.1 and 6.1 of the Regulation. The fact that advanced electronic signatures are already mentioned in the Regulation is a main advantage of this solution from a legal standpoint.</p> <p>As far as the qualified e-signature certificates used are compliant with the definitions provided in eIDAS, no major roadblocks are identified regarding the submission of statements of support in the form of an electronically signed PDF document.</p> <p>The characteristics and features that are required for the OCS to be certified by Member States' competent authorities are laid down in Article 6 of the Regulation. The statement of support generated with the PDF document will be adapted to include the e-signature, in accordance to Article 6.1.</p> <p>This solution is designed to ensure that only natural persons can complete the process, and the data to be retrieved from the PDF document will be stored in the same way as when users type in their data manually, complying with the two first conditions in Article 6.4.</p> <p>Regarding the last condition of Article 6.4, in order to provide statements of support in the forms compliant to Annex III, there is two possible scenarios:</p> <ul style="list-style-type: none"> ○ Annex III will be modified in order to include the possibility to sign with a qualified e-signature. ○ The users will need to complete the data not present in the e-signature certificate in order to comply with the current form of Annex III. <p>Under the first scenario, Annex III will be modified, including a separate form that foresees the use of e-signature. In this case, since the identity of</p>

			<p>the signatory could be verified with the data contained in the e-signature, users will not have to introduce any additional data into the system.</p> <p>On the contrary, in case there is no change in Annex III, each Member State's data requirement will need to be fulfilled. Therefore, users will have to complement the data stored in the certificate with other information required. Further analysis on this aspect can be found in section Quantity of data (input).</p>
Verification of statements of support	<p>Once the collection phase of an initiative has come to an end, organisers separate the statements of support collected in paper, in the OCS and those signed with e-signature and send them to the corresponding Member State verifying authorities.</p> <p>Verifying authorities receive the statement of support, and after verifying the identity of signatories, they shall certify the number of valid statements of support presented.</p>	<ul style="list-style-type: none"> ○ Art. 8.1 (ECI): organisers shall submit the collected statement of support, in paper or electronic form, to the relevant competent authorities for verification and certification. For that purpose, they shall use the form set out in Annex V, and separate the statement of support collected in paper, from those electronically signed, and those collected through an OCS. <p>Organisers shall submit statements of support to the relevant Member State as follows:</p> <ul style="list-style-type: none"> ○ To the Member State of residence or of nationality of the signatory, as specified in point 1 of Part C of Annex III, or ○ To the Member State that issued the personal identification number or the personal identification document indicated in point 2 of Part C of Annex III. <ul style="list-style-type: none"> ○ Art. 8.2 (ECI): The competent authorities shall verify the statements of support received on the basis of appropriate checks, in accordance with national law and practice. On that basis they shall deliver to the organisers a certificates (according to the model in Annex VI), certifying the number of valid statements of support, for the Member State concerned. 	<p>If this solution is implemented, statements of support submitted using e-signature will be sent online to the competent authorities, in accordance with art. 8.1. The form set out in Annex V will still be followed, separating all kinds of statement of support, with a specific section that will include the PDF documents signed electronically, as art.8.1 states. For this purpose, the use of e-signature can also be applied when representatives of the organiser's committee send the collected statements of support for verification.</p> <p>For this purpose, a modification of Annex V can be considered, in order to include a specific mention to the use of e-signature in the form that organisers have to comply with when carrying out this procedure</p> <p>Regarding the rules that determine which Member State the statements of support shall be submitted to, the Annex III will not be modified, and they will be sent to the corresponding verification authority according to the Certification Authority's Member State.</p> <p>In the light of the information displayed in the analysis, the verification of statements of support submitted using e-signature can be carried out within the current legal framework, and no modifications in the Regulation or the Annexes are required.</p>
Data protection and liabilities	<p>Once the PDF document is uploaded, the ones that contain personal data from signatories are stored in the OCS. Once the initiative is successful, those documents are destroyed.</p>	<ul style="list-style-type: none"> ○ Art. 5.3 (ECI) Signatories shall indicate only the personal data required for the purpose of verification by the Member States. ○ Art.12.1 (ECI): In processing personal data pursuant to this Regulation, the organisers of a citizens' initiative and the competent authorities of the Member State shall comply with Directive 95/46/EC and the national provisions adopted pursuant thereto. This reference to the Directive has to be understood as made to Regulation (EU) 2016/679, which repeals such Directive. 	<p>e-signature provides specific data that links the identity of the signatory to the specific statement of support signed. The information extracted from the e-signature certificate, and those fields that citizens may have to add will be, even in the worst-case scenario, equal to the personal requirements from Annex III. In accordance to Art 5.3, this solution will not require citizens to provide any extra information.</p> <p>The data that will be retrieved from the e-signature is only linked to the</p>

		<p>Art.12.2 (ECI): The organisers of a citizens’ initiative and the competent authorities shall be considered as data controllers, in accordance with the definition provided in Art.4 (7) of Regulation 2016/679.</p> <p>Art. 12.3 (ECI): The organisers shall ensure that personal data collected for a given citizen’s initiative are not used for any purpose other than their indicated support for that initiative, and shall destroy all statements of support received for that initiative and any copies thereof at the latest one month after submitting that initiative to the Commission or 18 months after the date of registration of the proposed citizens’ initiative, whichever is the earlier.</p> <p>Art. 12.4 (ECI): The competent authority shall use the personal data it receives for a given citizens’ initiative only for the purpose of verifying the statements of support and shall destroy all statements of support at the latest one month after issuing the certificate.</p> <p>Art. 12.6 (ECI): The organisers shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.</p>	<p>document signed and could not be used for other purposes. This fact reduces the legal risk that organisers and verifying authorities will face when managing personal information from citizen. Once the statements of support are validated and presented to the European Commission, organisers will destroy all of them within one month, or, 18 months after the collection phase has finalised, whichever is the earliest (art. 12. 3) No change in the way data is managed and destroyed is foreseen for this solution.</p> <p>The OCS will include all the necessary measures to ensure protection of such data, (Article 12.4) in order to obtain certification by the Member State’s competent authority where the server is located, as stated in Articles 6.1, 6.3 and 6.4.</p> <p>As long as the OCS is certified by the competent authority, this solution is compliant with the Regulation.</p> <p>Hence, organisers and verifying authorities will continue to comply with the regulation regarding data protection, although their legal risk will be mitigated due the fact that it is linked only to the statement of support, making it difficult to be used for other purposes.</p>
--	--	---	--

Table 34: Legal analysis, ECI Regulation - solution 1

13.2.2 Analysis of Member States' responses

The analysis of the situation of eID in the EU Member States is based on the information gathered through desk research as well as on the responses obtained from the questionnaires made available to representatives of each Member State. In total, 12 Member States shared their information:

- Austria
- Belgium
- Czech Republic
- Estonia
- Finland
- Germany
- Greece³⁹
- Luxembourg
- Netherlands
- Portugal
- Slovakia
- Spain

Key questions regarding the functioning of the ECI process and the current state of e-signature across the European Union were selected, extracting and processing the information in order to provide useful insights, aiming at assessing any possible roadblocks that this solution might face when implemented.

As mentioned, a key component of the proposed solution is the corresponding flag that will be stored in the OCS as a sign that the statement of support is produced with an electronically signed PDF document, the data being retrieved from the e-signature.

Question 1

Can we still continue with the current process within the Regulation, meaning the organiser sending the file of all their supporters to every national verification authority?

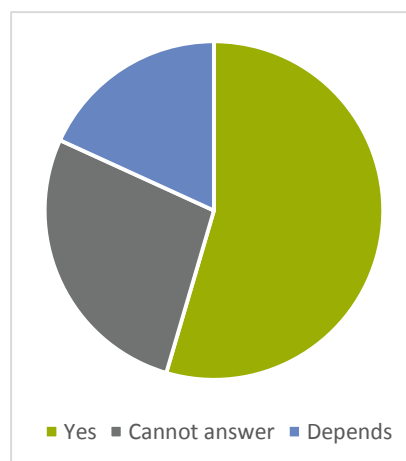


Figure 35: Responses from Member States. Question 1

As previously analysed, implementing solution 1 does not foresee any change in the procedure for verifying the statements of support, given the fact that no connection will be established directly with Member States' nodes. On the contrary, once the PDF documents are signed offline, they will be stored in the OCS and not delivered to verifying authorities until the end of the collection phase.

³⁹ DISCLAIMER: the information obtained from Greece was provided by a former representative that is awaiting to be replaced by the next appointed official. Therefore, the data regarding Greece cannot be considered as official.

The information extracted from this question reflects a common idea shared by most Member States: although statements of support could be considered as validated with the e-signature certificate, verifying authorities would be inclined to receive them and possibly perform proper validation checks in order to establish the identity of signatories.

Question 2

Could some of the personal data from Annex III be considered as optional?

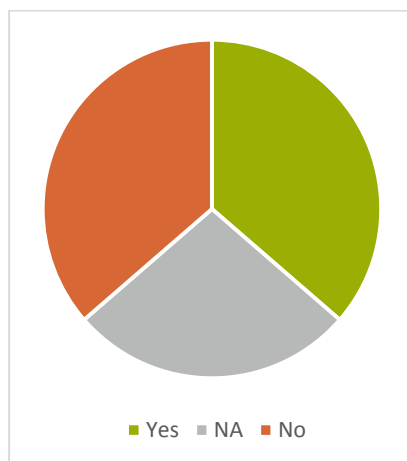
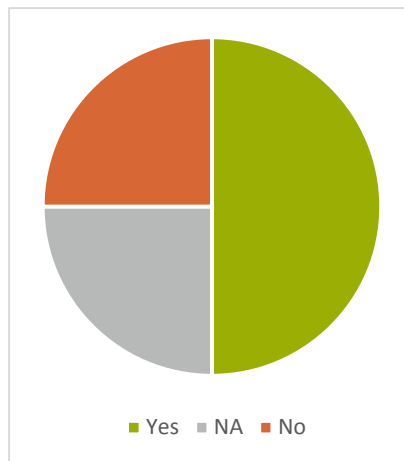


Figure 36: Responses from Member States. Question 2

When aiming at implementing this solution, the quantity of data that users will need to introduce manually is a key issue. Since solution 1 does not foresee a change in the ECI Regulation, a modification of Annex III has been proposed, in order to reduce the amount of data that users need to introduce, allowing citizens to validly create statements of support only with their e-signature certificates.

Regarding this question, the responses are more heterogeneous. More than a third of the Member States consulted were in favour of reducing the data requirements laid down in Annex III. However, at least another third indicates resistance to this possibility, while the rest could not provide an answer at the time of filling the questionnaire.

Question 3***Is e-signature enabled eID issued to a majority of the population?*****Figure 37: Responses from Member States. Question 3**

We can see from the responses gathered that approximately in half of the countries, e-signature certificates have been issued to the majority of population. Countries like Germany, Austria and Estonia reflected that e-signature certificates are already issued to all the population over 18 years old. From the countries whose answers were “no”, it’s important to stress that some of the Member States have indicated that the number of e-signatures issued is larger each year, proof of a growing trend across the EU.

In short, as reflected in question 1, Member States verifying authorities are willing to receive the statements of support in PDF, to perform checks and validate the identity of the citizen. This process is based on trustworthy data, as the information is retrieved from e-signature. Moreover, in order to simplify the process of submitting a statement of support, 30% of the consulted Member States are inclined to consider some data of Annex III as optional. Most Member States who answered our questionnaire confirmed that e-signature solutions are available in their country. The high penetration rate of e-signature in those countries can potentially contribute to a successful implementation of this solution. However, it should be noted that differences could be significant between the availability of e-signature solutions and the actual use of these tools by the citizens. Furthermore, some Member States, such as France and the Netherlands issue certificates to their citizens if they are representatives of legal persons, and other Member States do not issue any certificates at all. So in practice, the citizens of these Member States will be excluded from supporting ICE initiatives through this solution.

13.3 BUSINESS ANALYSIS**13.3.1 Ease of use****Citizens**

This solution does not speed up the process as it requires more steps to complete the submission of a valid statement of support. Furthermore, if the user has to go through the alternative flow 1, he/she has to fill the data requirements before downloading the PDF document, which results in a more complex and time-consuming process.

As explained in section 13.4.7, this solution's portability will allow users to carry out the procedure from a wide variety of web browsers. This fact has a positive impact on the ease of use, as different browsers can be chosen, providing a successful outcome when attempting to submit a statement of support using the electronically signed PDF.

Last but not least, it is also important to note that it might be possible that citizens do not have a supported e-signature certificate, depending on the availability of e-signature solutions and the degree of penetration in each Member State (see section 13.2.2), or that the certificate is no longer valid. Furthermore, the signatory must use a PDF reader software that supports the use of e-signature. If any of these conditions are not met, this alternative method for submitting a statement of support could not be completed.

In summary, citizens will benefit from a more secure system, although implementing this solution generally increases the time needed to finalise the process and adds complexity to the current way statements of support are submitted.

Campaign organisers

Regarding campaign organisers, the integration of e-signatures collected in PDF documents does not significantly change the way they manage the OCS platform and the data collected.

According to Article 8 of the Regulation, when submitting the statements of support to verifying authorities, organisers have to separate statements of support collected in paper, the ones collected through the OCS and those based on electronic signatures. As this procedure already foresees the use of e-signature, no change will be required if this solution is implemented.

Organisers will also benefit from this solution when sending statements of support for validation. As described in use case 2 (see section 4.1.1), the representative of the organisers' committee in charge of sending the statements of support to the corresponding verifying authorities will be able to use his/her e-signature when sending the form described in Annex V.

Consequently, no significant impact on the complexity of the OCS can be expected for campaign organisers regarding the collection phase. In addition, the possibility of using e-signature when delivering the collected statements of support brings added value to the process, by automating the procedure and fostering the use of electronic means to send such vital information.

Verifying Authorities

With regards to Member State's verifying authorities, the data contained in the e-signature can be extracted to allow an electronic validation by cross-checking with their national citizens' register. When applying a qualified electronic signature, the certificate containing the citizen identification data is included in the e-signature, which guarantees its integrity and correctness. The identification data contained in certificates is very stable and allows identifying the citizen during the entire validity period of a certificate.

To sum up, e-signature improves the quality of online statements of support, easing the task of validation and the issuing of the certificate (according to the model set out in Annex VI of the Regulation) that accounts for the number of valid statement of support received.

13.3.2 Quantity of data (input)

Citizens

Qualified e-signatures contain data that enable the identification of a user. However, as mentioned in section 4.1.1, validation of e-signatures will depend on the different implementation paths that this Solution might follow.

Under the basic flow scenario (see use case 1, section 4.1.1), statements of support are validated with no additional data beyond the one from the certificate, reducing the quantity of data inserted manually by the user to zero. Within the alternative flow 1, users will still need to type in some of the data, although a large quantity of the data required will be already present in the e-signature certificate.

Campaign organisers

Campaign organisers will be positively affected regarding the data they manage under the current OCS, especially regarding protection of such data. Organisers are considered as data controllers under Regulation (EU) 2016/679, (repealing Directive 95/46/EC, mentioned in the ECI Regulation) during the initiative's collection phase (Article 12, paragraph 2 of the ECI Regulation), being held responsible for any damage they cause (Article 13). The integrity and correctness of the data contained in e-signatures enhance security and reduce the legal risks that organisers currently face.

In addition, implementing this solution will help organisers for the purpose of planning and managing the campaign: nowadays, they are recommended to obtain an extra 20% statements of support in order to account for invalid ones⁴⁰. Since statements of support based on e-signatures provide high confidence in their later validation, they will give organisers better idea of the number of valid statements collected so far.

Verifying Authorities

The impact for Member State's verifying authorities on the amount of data managed could be significant, especially if they agree to consider statements of support based on e-signature as validated with no additional data requirements. If this solution is implemented, verifying authorities will be able to establish the identity of signatories only by checking the validity of the e-signature certificate.

If the certificate was valid when the statement of support was submitted, the identities will not have to be verified again, easing the task of checking the data against national databases, and against duplicates (statements of support submitted by the same user with different certificates. This simplification could eventually lead to a reduction in the amount of data verifying authorities would deal with. This reduction on the amount of statements of support that need to be validated relieves the burden of verifying authorities. However, it should be noted that if advanced electronic signatures are allowed (and not only qualified electronic signature), the risk of fraud will be higher in

⁴⁰ Le Gouvernement du Grand-Duché de Luxembourg (2015) *Potential Benefits Of Electronic Signatures in The Context of European Citizen Initiatives*. p.2

case someone having access to the database decides to fraudulently reuse the certificates generated by an advanced e-signature to sign statements of support in other peoples' names.

13.3.3 Penetration of the solution / awareness

Citizens

As mentioned, different e-signature certificates have been put in place across the Member States. Therefore, the level of penetration of this solution is quite heterogeneous. The research carried out so far shows that not all countries use the same type of electronic signature. Furthermore, whereas in some countries e-signature is becoming a widely-used tool, in others, its penetration is not yet significant.

In the Member States where a national eID card system has been put in place and the smart cards have already been issued to a vast majority of the adult population (Belgium, Germany, Italy, Spain, etc.), the eID cards usually contain certificates allowing the use of e-signature. Accordingly, the impact of this solution will be higher than in the Member States where e-signatures are not widely penetrated. This impact should however be mitigated in light of the difference between the level of penetration and the actual usage of e-signatures across the Member States.

There is another important remark to be made regarding the type of certificates used. Qualified certificates are issued under supervision of the national competent authorities for eID, and comply with the national requirements regarding completeness, correctness and integrity of the data. The main benefit of using qualified certificates is that these certificates identify the citizen to whom it was issued, and furthermore they are trusted.

On the other hand, it should be noted that if the requirement of qualified certificates was to be extended to all Member States, this solution would exclude Member States such as France and the Netherlands which issue certificates only to representatives of legal persons, and other Member States which do not issue any certificates. Leaving the qualified signatures as recommended instead of required, would not exclude any Member State: in all Member States non-qualified certificates are present, although in certain ones within a limited degree of penetration.

A special category of certificates is formed by those certificates that are not held by the subscriber, like the mobile solutions in Austria: these certificates are stored in an HSM (Hardware Security Module) to which physical and logical access is restricted and monitored. Access to the certificate is granted if the user introduces the access codes. These certificates can only be used for producing signatures, i.e. are valid for this solution but not for authentication: not any browser supports sending the seed to be signed elsewhere, nor do signing functions support visualising such a seed.

According to the information presented in section 13.4.6, the maturity of this solution provides an ideal implementation scenario, as all the technical components of this solution are available and ready to be put to function.

In light of the information presented, and given the feedback received from Member States, we can conclude that the penetration of this solution is remarkable, given the fact that PDF documents are widely used, that e-signature is a tool that has been used for many years, and its use is now very extended across the EU. Indeed, half of the consulted countries mentioned that e-signature certificates have been issued to the majority their population. Moreover, the number of issued e-

signature certificates is larger each year, emphasising this growing trend across the European Union (see section 13.2.2).

Campaign organisers

From the point of view of the organisers, the possibility of adding additional features to the OCS that may make the ECI process more user-friendly and attractive to the general public can have a positive impact, as it will be easier for them to raise awareness about their campaign and gather a larger number of statements of support.

The reduced legal risks (see sections 13.2.1 and 13.3.2) and enhanced user interface may attract more interested citizens to become organisers and campaign for any given cause. However, such effects will be in any case indirect, and difficult to assess individually.

Verifying Authorities

Regarding this specific criterion, verifying authorities will notice a significantly positive impact. Since the e-signature certificates selected for integration into the OCS are generally the most used ones in each Member State, it is likely that verifying authorities will trust the information retrieved from those certificates. Hence, the verification task will be facilitated, as the ratio of valid statements of support should be higher.

13.4 TECHNICAL ANALYSIS

13.4.1 Ease of integration

Changes in the navigation in the OCS

The navigation in the OCS system will need some changes, such as the inclusion of a button to download the PDF document and a second one to upload the signed document. Additionally, the actions corresponding to the user's clicks on these buttons must be included. These are considered minor changes, which will not present any problems to integrate.

Inclusion of PDF support in the OCS

This solution requires the inclusion of PDF manipulation support for the inclusion and extraction of data in the fields of a PDF document, as well as for the extraction of the signature. Although such software could be custom developed, it is highly recommended to use available standard libraries to reduce the cost of development and increase the reliability of the solution. Some of the highlighted options are:

- Adobe PDF Library, with Proprietary license
- Poppler, with GNU GPL license
- PDFBox, with Apache license
- iText, with AGPL license

Considering the completeness of the solution and guarantees offered for correct functioning, the Adobe libraries are the preferred option. However, its licensing policy is not compatible with the EC and Member State licensing policies, which prefer European Union Public License (EUPL).

Considering the license type, the most adequate appears to be Poppler, which is compatible with EUPL licensing. While this library supports C++ as programming language, the EU preference of using Java as programming language is not supported.

Considering experiences in EU co-financed projects, the iText solution should be preferred; the STORK project has successfully deployed a solution for manipulation of PDF documents, including contents of fields, signing the document and extracting the signature. Its main drawback is the licensing: AGLP is more requiring than EUPL. Furthermore EUPL is admitted in courts of justice in the EU; with other license type there is less experience.

In conclusion, previous experience with the inclusion of PDF manipulation (e.g. pilot 5 (Change of Address) of the STORK project) has demonstrated that PDF manipulation libraries of iText are easy to integrate.

Inclusion of a certificate validation module

This solution proposes the inclusion of a certificate validation module, in charge of a basic validation:

- The validity period of the certificate: the timestamp `notBefore` should be inferior to the system date/time, and the timestamp `notAfter` should be superior to it.
- The membership of the EU of the issuing CA: the value of the “C” attribute of the issuer of the certificate must be in a list of the 28 Member States
- The issuer of the certificate must be mentioned in the TSL of the Member State
- The certificate must be issued to a natural person: if the Member State issues certificates to legal persons, the OID must be present in the list of OIDs for natural persons for this specific Member State.
- The certificate must be enabled for signing (`keyUsage` includes `contentCommitment`)

This module is more or less complex: the function of interpreting the different TSLs is especially complex. However, as there is only one module like that, the over-all complexity is considered moderate.

13.4.2 Scalability

As mentioned, the OCS is extended with one custom-built module, in charge of the validation of the certificate used for signing, as described in the previous section.

This module could need a change in its configuration in case new Member States would be included in the EU; this does not entail any scalability issue.

The PDF manipulation module does not present any scalability issues: any change in the amount of supported eIDs or their formats has no impact on this module.

13.4.3 Maintainability

The maintainability is expected not to produce any major problems: the PDF and PAdES specifications are not expected to change, and the specifications of the Trusted Lists are not expected to change either. Consequently, the software supporting these specifications can be expected to be stable, not provoking any maintainability issues.

13.4.4 Performance and usage of resources

This solution has an impact on the resources, especially on disk usage: the increase of disk space needs is due to the fact that a signed PDF document occupies more space than the user's data in a database: for a signed PDF, an estimated size is around 50KB, while the disk occupation of user's data may be estimated to 1-5KB, depending on the amount of indexes, enabled tracing and auditing facilities, etc. The total increase of disk space for a successful initiative, supposing that 20% of the 1,000,000 statements of support would use this solution would be 10 GB.

13.4.5 Security

Security on data storage

As far as the current security measures for the OCS meet ECI framework requirements, i.e. the requirements of the Regulation, as well as the ones reflected in the ECI technical specifications, no further changes are foreseen for the data stored in the OCS database. These measures should also be applied to the two new columns in the database.

Additional to the current security measures, the signature guarantees the integrity of these documents: any change in the document would invalidate the signature.

The protection of these documents against loss can be guaranteed by a normal back-up procedure. The parameters of this procedure need to be verified to include new columns in the database.

In summary, security of the data stored will not be compromised by the changes that will be made in the OCS if this solution is implemented.

Security of data transmissions

The data transmissions between the OCS and the citizen use a secure channel (SSL or TLS), so the confidentiality is guaranteed by the encryption used in this channel. The integrity of the transmission is achieved with the e-signature in the PDF document.

Currently the procedure for transmission of statements of support from the organisers to the verifying authorities is heterogeneous: each Member State has its own procedure. This study proposes a homogeneous procedure, described in 13.1.2, in order to facilitate this task for the organisers. The security measures in this procedure are:

- The compacted set of PDF documents is encrypted, e.g. with AES, in order to guarantee its confidentiality while being stored on a file server available to the internet
- The integrity of the compacted file is guaranteed by the compacting mechanism
- The link to the file and its decryption key are sent by email to the verifying authorities by secure email.

With this procedure the security of this transmission is guaranteed, if the quality of the encryption meets industry standards, e.g. using AES-256⁴¹.

⁴¹ AES proposal: Rijndael: <http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf#page=1>

Session management

Http is a “stateless” protocol, i.e. all transactions are fully independent of previous transactions. The critical time for session management is the period between sending a statement of support to the OCS and the confirmation of support by the user. These two sessions are linked to each other by using a cookie; most Java application servers use the variable JsessionID, whose value determines the thread to which the http request is passed in order to handle it. This variable should be transmitted as a cookie, with the http-only clause, in order to avoid session hijacking.

The vulnerable point is the relation between the uploaded PDF document and the confirmation of support. Apart from the mentioned cookie, no special measures can be applied, nor are they required.

Fraud prevention

e-signatures cannot be produced without the explicit agreement of the subscriber of the certificate used for producing the e-signature. Thus, in the case qualified certificates are stored on qualified signature creation devices, it is impossible to sign a PDF with a qualified certificate on behalf of other persons. Fraud could only take place if a certificate stored on non-secure device is compromised, and limited in time until its revocation. The OCS easily detects copied PDF documents: the certificate used in both PDF documents would be the same.

The usage of signed PDFs offers no on-line solution for detection of non- EU citizens residing in the EU, neither does it provide measures for avoiding that people support the same initiative twice, using different certificates, certificates from different Member States or different methods for supporting (paper, traditional OCS, etc.).

Vulnerability for DoS

This solution introduces a vulnerability with Denial of Service: whereas PDF documents are not big, the verification of the signature entails a possibility of overloading the server’s CPU. This risk can be mitigated by forbidding multiple connections from the same IP address, but such measure would not mitigate the risk of a DDoS (Distributed Denial of Service). Furthermore, controls can be put in place to limit the size of the PDF documents to prevent DoS because of bulky PDF upload.

13.4.6 Maturity

Since the European signature directive (1999/93/EC) and its adoption in the legislation of all EU Member States, electronic signatures have become normal use in applications which require content commitment. The standards used in this solution with signed PDF documents are completely mature:

- PDF is the most commonly used standard for document exchange on the Internet
- PAdES is the commonly accepted standard for signatures on PDF documents
- Most PDF readers support producing advanced signatures on documents
- Up and downloads of files are common practice

13.4.7 Portability

The current implementation of the OCS uses Java as a programming language: the adaptation to be made must also use the Java development platform in order to allow an easy integration. Java is portable to all commonly used operating systems; mostly it does not even require a recompilation. Java source can be used with most current versions of common application servers, like Tomcat,

Glassfish, JBoss, WebLogic and WebSphere. However, a solution built on one of the application servers will likely need a porting in order to be used on other application servers too.

This solution entails no special issues for usage on other devices than PCs, portable devices like tablets and smartphones: the only requirement is that, if the signing certificate is stored in a cryptographic device, the portable device should be enabled to read the cryptographic device. Several Member States have already implemented solutions for usage of their eIDs, like the mobile solutions in Austria and Estonia, or the German nPA and version 3.0 of the Spanish DNle, which use contactless technologies for this purpose.

13.4.8 Costs / efforts

The efforts required for inclusion of signed PDF documents in OCS can be split among the required changes:

- Changes in the navigation: around 1 man-month
- Inclusion of the PDF manipulation: around 2 man-months
- Inclusion of a certificate validation module: around 2 man-months

These estimations consider dividing common efforts, like documentation of the design, system tests, etc., between these three changes. So a first estimation of the required efforts would be around 5 man-months.

14 APPENDIX C – SOLUTION 2: E-SIGNATURE

14.1 DETAILED DESCRIPTION

A European citizen supports an initiative. To prove his/her identity, he/she presents his/her eID to the OCS website, with the national eID enabled for authentication. This description supposes that the signature tool is already installed on the user's PC. However, a Webstart signature tool (or similar), not requiring a prior installation, might also be used.

14.1.1 Use Case 1: Collection of statements of support

The steps to submit a statement of support using e-signature are detailed in the following use case:

e-signature	
Name	Creation of an electronically signed statement of support
Description	The user supports an initiative using an e-signature
Actor (Generic)	EU citizen with the right to vote for the EP
Preconditions	The user has a valid e-signature certificate available
Basic flow	<p><u>Integration with e-signature</u></p> <p>The user:</p> <ol style="list-style-type: none"> 1. Accesses the ECI website 2. Selects a specific initiative to support 3. Clicks on the "Support" button 4. In the data-filling webpage, selects his/her country 5. Selects the option to use e-signature 6. Selects the certificate 7. If the certificate is stored in a cryptographic device, the user enters the PIN 8. Confirms the submission of the statement of support
Alternative flow 1	<p><u>e-signature with the user filling his/her data</u></p> <p>The user:</p> <ol style="list-style-type: none"> 9. Accesses the ECI website 10. Selects a specific initiative to support 11. Clicks on the "Support" button 12. In the data-filling webpage, selects his/her country 13. Selects the option to use e-signature 14. Selects the e-signature certificate 15. If the certificate is stored in a cryptographic device, the user enters the PIN 16. Fills the missing data if necessary 17. Confirms the submission of the statement of support
Exception flow	<p>The certificate is no longer valid, revoked or cannot be read</p> <p><u>Resolution:</u> statements of support can be submitted by manually typing data into the OCS</p>

Devices	<ul style="list-style-type: none"> • Computer • As far as the certificate is stored in a card, a card reader must be connected to the computer
Software	Supported Internet browser

Table 35: Use case - integration of e-signature

Depending on the technical implementation possibilities to accept statements of support signed under this use case, the implementation of this solution will follow different paths.

The ideal scenario described in the basic flow assumes that statements of support will be validated with the data contained in the e-signature certificate only, without requiring any additional data. Alternatively, if this solution follows a different implementation path, the alternative flow is a viable option, where users have to enter the additional data not stored in their e-signature certificates.

Actors

Abbreviation	Description
Citizen	A European citizen, with the right to vote in elections for the European Parliament, willing to support an initiative
Browser	A software tool designed to navigate web pages on the Internet
Sign tool	A software tool, integrated with the browser, designed to create e-signatures on contents of the html page, and return this signature to the same page. An example of such signature tool is the one published in the EC's Joinup portal ⁴²
OCS	Online Collection System. A system designed to collect statements of support for initiatives.
MS validation	External system used for validation of the status of certificates. One of the most used methods is the publication of a CRL, while OCSP is less popular ⁴³ .

Table 36: Actors for collection of statements of support

Activity diagram

The following diagram illustrates the actions and dataflows between the involved parties in the collection phase.

⁴² SD-DSS solution at the Joinup portal: <https://joinup.ec.europa.eu/software/sd-dss/release/all>

⁴³ A Member State may not always offer such validation services. To overcome this problem, the DSS tool is able to perform the validation of an e-signature by itself.

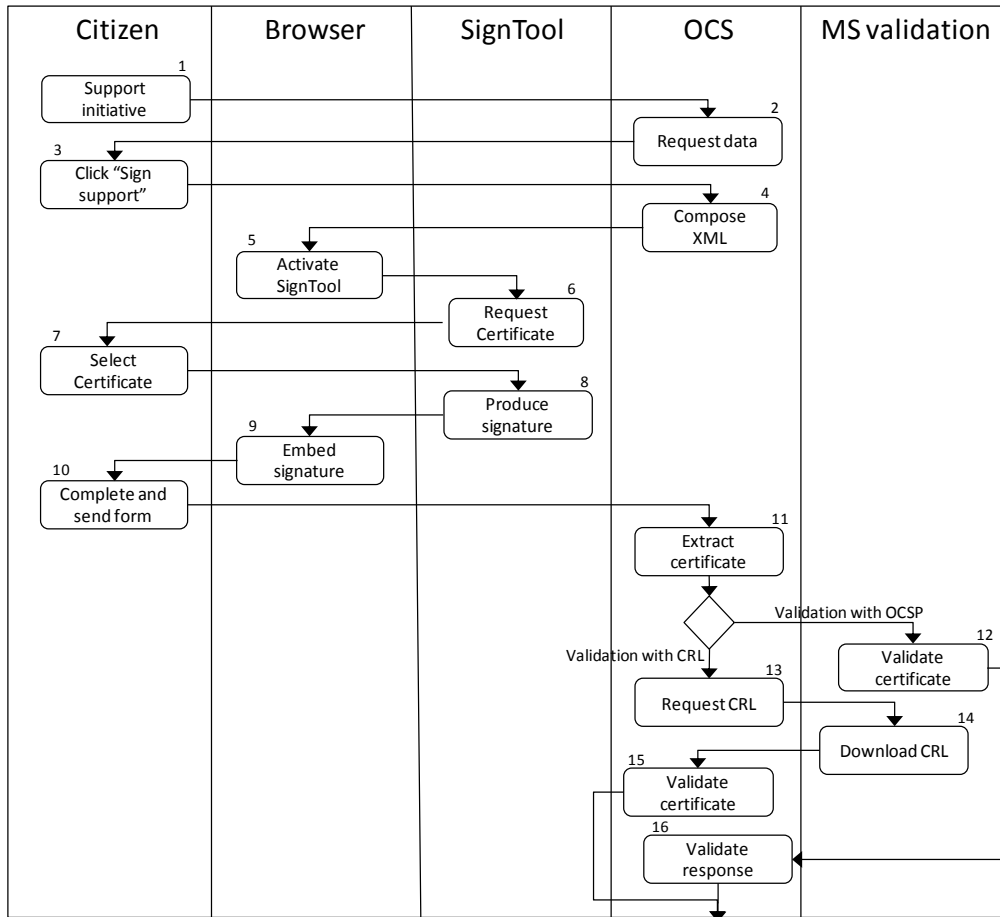


Figure 38: Activity diagram of the collection process – part 1

Action ID	Actor	Description
1	Citizen	Support initiative The citizen decides to support an initiative. After going through the details of the initiative, the button “Support” on the final informative page leads to the OCS.
2	OCS	Request data The OCS presents a page where the user is requested to indicate his home country, and depending on this country he/she is requested to fill his personal data. This page also presents a button “Sign support”. Please note that on this page there is one more button: “Support” which leads to the traditional OCS functionality. There could also be some other buttons, corresponding to other ways to support this initiative. These options are irrelevant in this chapter.
3	Citizen	Click “Sign the statement of support” The citizen clicks the button “Sign the statement of support”.
4	OCS	Compose XML The OCS composes the XML structure to be signed. This structure

		contains the name of the initiative to be supported. The html code includes the code to activate the sign tool.
5	Browser	Activate Sign tool The browser activates the sign tool, in order to produce the signature on the received XML structure, and to return the signature in the html page
6	Sign tool	Request certificate The sign tool requests the citizen to select his certificate in order to produce a signature.
7	Citizen	Select certificate The citizen selects the certificate the Sign tool should use for producing the signature.
8	Sign tool	Produce signature The Sign tool uses the private key associated with the selected certificate to produce the signature, embedded in the XML structure (standards XAdES signature).
9	Browser	Embed signature The browser embeds the signed XML structure in the html page in the contents of the prepared hidden field.
10	Citizen	Complete and send form The citizen fills the required fields. Considering that the citizen is completely identified by his qualified certificate, these additional fields should be his nationality and for some Member States his date of birth. Next he/she clicks the "support" button to send the form to the OCS.
11	OCS	Extract certificate The OCS validates the signature and extracts the certificate used for signing from the XML structure. The OCS validates this certificate with some basic checks. These basic checks include: <ul style="list-style-type: none"> • Validity, according to the validity period: notBefore and notAfter are compared with the current system time • If the certificate is issued in a EU Member State: the "C" attribute of the issuer of the certificate is compared with the list of 28 Member States • If the issuer is mentioned in the TSL of its Member State, thus the certificate is qualified • If the certificate is enabled for signing (keyUsage includes contentCommitment) • If the certificate is issued to a natural person (the OID is included in a list of OIDs of natural persons for the

		<p>corresponding Member State</p> <p>Depending on the required method of validation the flow continues with activity 12 for OCSP or activity 13 for CRL.</p>
12	MS validation	<p>Validate certificate</p> <p>The validation service of the Member States' CA (OCSP) validates the certificate and the e-signature, and returns its status: active, suspended or revoked.</p> <p>This response is sent to activity 16.</p>
13	OCS	<p>Request CRL</p> <p>The OCS requests the MS validation service to send the CRL. Please note that CRLs are not updated frequently, so this activity could be performed periodically, e.g. every hour.</p>
14	MS validation	<p>Send CRL</p> <p>The MS validation sends the CRL. Please note that CRLs are not updated frequently, so this activity could be performed only if a new CRL is present. In that case the CRL is stored on the server's local disk. If the CRL is a complete CRL, it substitutes the previous CRL.</p>
15	OCS	<p>Validate certificate</p> <p>The OCS verifies if the certificate used for signing is mentioned explicitly or implicitly in the CRL. If the CRL is a partial one, all previous CRLs are checked, until a complete CRL is found.</p>
16	OCS	<p>Validate response</p> <p>The OCS verifies that the OCSP response is signed by the competent authority, i.e. the certificate used for signing it is issued with the same root certificate as the root certificate of the citizen's certificate.</p>
17	OCS	<p>Extract data</p> <p>The OCS extracts the citizen's data from the certificate.</p>
18	OCS	<p>Request confirmation</p> <p>The OCS fills the citizen's data in the final support form, requesting the citizen to confirm his support to the current initiative.</p>
19	Citizen	<p>Confirm support</p> <p>The citizen clicks the "Confirm support" button.</p>
20	OCS	<p>Store support</p> <p>The OCS stores this statement of support in its database. And confirms the support to the citizen.</p>

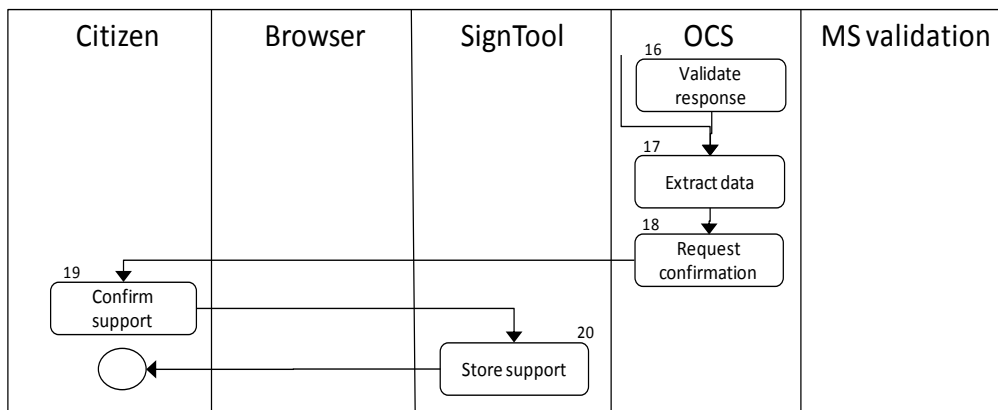


Figure 39: Activity diagram of the collection process – part 2

Activity 11 should be highlighted, as it is far more complex than its name suggests:

Extract certificate

The OCS validates the signature and extracts the certificate used for signing from the XML structure.

The OCS validates this certificate with some basic checks. These basic checks include:

- Validity, according to the validity period: notBefore and notAfter are compared with the current system time
- If the certificate is issued in a EU Member State: the “C” attribute of the issuer of the certificate is compared with the list of 28 Member States
- If the issues is mentioned in the TSL of its Member State, thus the certificate is qualified
- If the certificate is enabled for signing (keyUsage includes contentCommitment)
- If the certificate is issued to a natural person (the OID is included in a list of OIDs of natural persons for the corresponding Member State)

14.2 OVERVIEW OF THE LEGAL FRAMEWORK

14.2.1 Analysis of the ECI Regulation

	Solution 2- Description	Requirements (ECI)	Review
Submission of statements of support	<p>Solution 2 is based on an integration between the OCS and the e-signature service provider of each Member State. Citizens will make use of their e-signature certificates to sign the statement of support. The OCS will connect to the corresponding Member State node in order to extract the information and store it in its database.</p>	<ul style="list-style-type: none"> ○ Art. 5.1(ECI): only forms that comply with Annex III may be used for the collection of statements of support. ○ Art. 5.2 (ECI): statements of support may be collected in paper form or electronically. Statement of support signed with advanced electronic signatures shall be treated in the same way as those submitted in paper form. ○ Art. 6.1(ECI) the OCS shall be certified in accordance with Article 6.3 by the competent authority of the Member State in which the data will be stored The models for the statement of support forms may be adapted for the purpose of the online collection ○ Art. 6.2 (ECI): The OCS shall be compliant with the conditions stated in Article 6.4. ○ Art. 6.3 (ECI): the relevant authorities shall issue a certificate (according to the model set out in Annex IV) confirming the OCS complies with the requirements of Art. 6.4. ○ Art. 6.4 (ECI): Online collection systems shall have the adequate security and technical features in order to ensure that: <ul style="list-style-type: none"> ○ only natural persons may submit a statement of support; ○ the data provided online are securely collected and stored, in order to ensure, inter alia, that they may not be modified or used for any purpose other than their indicated support of the given citizens' initiative and to protect personal data against accidental or unlawful destruction or accidental loss, alteration or unauthorised disclosure or access; ○ the system can generate statements of support in a form complying with the models set out in Annex III, in order to allow for the verification by the Member States in accordance with Article 8(2) 	<p>Solution 4 will follow the dictate of Article 6 by adapting the form in Annex III of the Regulation for the purpose of submitting a statement of support in an online form. The fact that advanced electronic signatures are already mentioned in the Regulation (Article 5.2) is a main advantage of this solution from a legal standpoint.</p> <p>As far as the e-signature certificates used are compliant with the definitions provided in eIDAS for qualified certificates and signatures, this solution is feasible within the Regulation.</p> <p>The main features required for the OCS to be compliant with the Regulation are listed in Article 6. By establishing a connection to the Member State's certificate validation services, the OCS will be able to connect all the required information regarding a signatory, being able to ensure a secure connection and storage, and that only natural persons' data is used to create statements of support. The data will be stored in the same way as it is currently done, ensuring that it does not suffer from unlawful use, loss or destruction.</p> <p>Regarding the last condition of Article 6.4, in order to provide statements of support in the forms compliant to Annex III, a modification of Annex III is proposed, in order to include an additional form of the statement of support that is created with the data included in the e-signature certificate.</p> <p>Under the first scenario, Annex III will be modified, including a separate form that foresees the use of e-signature. In this case, since the identity of the signatory is known with the data contained in the e-signature, users will not have to introduce any additional data into the system.</p>
Verification of statements of	<p>Once the collection phase of an initiative has come to an end, organisers separate the statements</p>	<ul style="list-style-type: none"> ○ Art. 8.1 (ECI): organisers shall submit the collected statement of support, in paper or electronic form, to the relevant competent authorities for verification and certification. For that purpose, they shall use the form set out in Annex V, and 	<p>If this solution is implemented, statements of support submitted using e-signature will be flagged with an indicator that will be proof of a validation of the data from national databases. It would be advisable to amend</p>

<p>support</p>	<p>of support collected in paper, in the OCS and those signed with e-signature and send them to the corresponding Member State verifying authorities.</p> <p>Verifying authorities receive the statement of support, and after verifying the identity of signatories, they shall certify the number of valid statements of support presented.</p>	<p>separate the statement of support collected in paper, from those electronically signed, and those collected through an OCS.</p> <p>Organisers shall submit statements of support to the relevant Member State as follows:</p> <ul style="list-style-type: none"> ○ To the Member State of residence or of nationality of the signatory, as specified in point 1 of Part C of Annex III, or ○ To the Member State that issued the personal identification number or the personal identification document indicated in point 2 of Part C of Annex III. <p>○ Art. 8.2 (ECI): The competent authorities shall verify the statements of support received on the basis of appropriate checks, in accordance with national law and practice. On that basis they shall deliver to the organisers a certificates (according to the model in Annex VI), certifying the number of valid statements of support, for the Member State concerned.</p>	<p>Article 8 in order to include the automatic validation of data coming from e-signatures, with a flag that will account for those statements of support that have been already validated. Besides, the format of the flag that will be created and stored with the data retrieved should be properly defined, preventing a possible tampering of such data or any unlawful use of it.</p> <p>Even though a validation will be carried out on the spot when the OCS accesses the corresponding national database, statements of support will be delivered to the competent authorities, in accordance with art.8.1. Following the mandate of this Article, the different categories of statements of support will be separated (statements of support signed in paper, in the OCS by typing the personal data and via e-signature)</p> <p>Regarding the Member State to which those statements of support shall be submitted to, the Annex III should be modified by adding a specific criterion for the statements of support submitted via e-signature. Those statements of support should be sent to the country in which the e-signature certificate was issued, in case national authorities wish to carry out further validation or check for duplicates.</p> <p>The rest of statements of support are sent to the corresponding Member State, according to the criteria of residence/nationality and Member State issuing the personal identification number.</p>
<p>Data protection and liabilities</p>	<p>Once the PDF document is uploaded, the PDF documents that contain personal data from signatories will be stored in the OCS system. Once the initiative becomes successful, those documents will be destroyed.</p>	<ul style="list-style-type: none"> ○ Art. 5.3 (ECI) Signatories shall indicate only the personal data required for the purpose of verification by the Member States. ○ Art.12.1 (ECI): In processing personal data pursuant to this Regulation, the organisers of a citizens’ initiative and the competent authorities of the Member State shall comply with Directive 95/46/EC and the national provisions adopted pursuant thereto. This reference to the Directive has to be understood as made to Regulation (EU) 2016/679, which repeals such Directive. ○ Art.12.2 (ECI): The organisers of a citizens’ initiative and the competent authorities shall be considered as data controllers, in accordance with the definition provided in Art.4 (7) of Regulation 2016/679. ○ Art. 12.3 (ECI): The organisers shall ensure that personal data collected for a given citizen’s initiative are not used for any other purpose than their indicated support for that initiative, and shall destroy all statements of support received for that initiative and any copies thereof at the latest one month after submitting that 	<p>e-signature provides specific data that includes the identity of the signatory and links to the specific statement of support signed. The information extracted from the e-signature certificate will be always less or equal to the personal requirements from Annex III. In accordance to Art 5.3, this solution will not require citizens to provide any extra information.</p> <p>The data that will be retrieved from the e-signature is specifically linked to the statement signed and could not be used for other purposes. This fact reduces the legal risk that organisers and verifying authorities will face when managing personal information from citizen. Once the statements of support are validated and presented to the European Commission, organisers will destroy all of them within one month, or, 18 months after the collection phase has finalised, whichever is the earliest (art. 12. 3) No change in the way data is stored and later destroyed is foreseen for this solution.</p> <p>All necessary features in order to ensure protection of personal data will be included in the OCS, (Art. 12.4) aiming at obtaining certification by the corresponding MS authority, in accordance with Arts. 6.1, 6.3 and 6.4. As long as the OCS is certified by the competent authority, this solution will</p>

		<p>initiative to the Commission or 18 months after the date of registration of the proposed citizens' initiative, whichever is the earlier.</p> <ul style="list-style-type: none"> ○ Art. 12.4 (ECI): The competent authority shall use the personal data it receives for a given citizens' initiative only for the purpose of verifying the statements of support and shall destroy all statements of support at the latest one month after issuing the certificate. ○ Art. 12.6 (ECI): The organisers shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. 	<p>be compliant with the Regulation.</p> <p>Hence, organisers and verifying authorities will continue to comply with the Regulation regarding data protection. In addition, their legal risk will be mitigated due to the encryption of the e-signature data and the fact that it is linked uniquely to the statement of support, making it difficult to be used for other purposes.</p>
--	--	--	--

Table 37: Legal analysis, ECI Regulation - solution 2

14.2.2 Analysis of the eIDAS Regulation

Regarding the use of e-signature eIDAS establishes a whole new regulatory framework, substituting previous directives.

This solution foresees the possibility to allow the use of qualified electronic signatures, given the fact that they provide the highest level of assurance regarding the identity of the person signing an initiative. The eIDAS Regulation also establishes an unambiguous legal value for electronic signatures that is different for the various categories.

All Member States shall follow this standard, as the eIDAS Regulation has direct effect on their territories. The following table provide a comprehensive review on qualified electronic signatures, trust services and the legal value of e-signatures:

Scope	
<p>Art. 1: With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:</p> <p><i>“Establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.”</i></p>	
Definitions (e-signature and trust services)	
Qualified electronic signatures	Trust services
<p>Art. 3 (12): <i>‘qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. Article 28 states that the qualified certificate shall comply with the requirements laid down in Annex I:</i></p> <ul style="list-style-type: none"> • <i>an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;</i> • <i>a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:</i> • <i>for a natural person: the person’s name;</i> • <i>at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;</i> • <i>electronic signature validation data that corresponds to the electronic signature creation data;</i> • <i>details of the beginning and end of the certificate’s period of validity;</i> • <i>the certificate identity code, which must be unique for the qualified trust service provider;</i> • <i>the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;</i> • <i>the location where the certificate supporting the advanced electronic signature or advanced electronic seal</i> 	<p>Art. 3(16): ‘trust service’ means an electronic service normally provided for remuneration which consists of:</p> <ul style="list-style-type: none"> (d) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services (e) the creation, verification and validation of certificates for website authentication; or (f) the preservation of electronic signatures, seals or certificates related to those services; <p>Art.3 (17): ‘qualified trust service’ means a trust service that meets the applicable requirements laid down in this Regulation</p> <p>Art. 3(19): ‘trust service provider’ means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;</p> <p>(20) ‘qualified trust service provider’ means a trust service provider who provides one or more qualified trust services and is gr</p> <p>Art. 22.1: Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.;</p> <p>2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.</p> <p>3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.</p>

<p><i>referred to in point (g) is available free of charge;</i></p> <ul style="list-style-type: none"> • <i>the location of the services that can be used to enquire about the validity status of the qualified certificate;</i> <p><i>(j) Where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.</i></p>	
---	--

Table 38: Legal analysis, eIDAS Regulation - solution 2

As mentioned, this solution foresees the use of qualified signatures, since they provide the highest degree of confidence in the identity of the person signing the statement of support. Besides, qualified certificates are only issued by qualified service providers, who are under strict control of Member States through national laws and trusted lists. Therefore, these are ideal tools to be integrated into the OCS, providing secured and trustworthy data that verifying authorities will be able to validate without further checks.

The research carried out has concluded that all Member States have published and updated trusted lists, and therefore qualified electronic signatures are issued all across the EU. The fact that the selected eIDs are already penetrated across Member States increases the probability of a successful implementation and the establishment of a new procedure to create statements of support that is secure and compliant with the eIDAS Regulation. However some Member States do not issue signature certificates to their complete population, e.g. France and the Netherlands only issue certificates to representatives of legal persons; other countries have other limitations to issuing certificates to their population.

Besides, the legal value granted to qualified electronic signatures provides safe grounds for organisers and verifying authorities to comply with their task with no legal risks associated.

14.2.3 Analysis of Member State Responses

The analysis of the situation of eID in the EU Member States is based on the information gathered through desk research as well as on the responses obtained from the questionnaires made available to representatives of each Member State. In total, 12 Member States shared their information:

- Austria
- Belgium
- Czech Republic
- Estonia
- Finland
- Germany
- Greece⁴⁴
- Luxembourg
- Netherlands
- Portugal
- Slovakia
- Spain

Key questions regarding the functioning of the ECI process and the current state of e-signature across the European Union were selected, extracting and processing the information in order to provide

⁴⁴ The information obtained from Greece was provided by a former representative that is awaiting to be replaced by the next appointed official. Therefore, the data regarding Greece cannot be considered as official.

useful insights, aiming at assessing any possible roadblocks that this solution might face when implemented.

As mentioned, a key component of the proposed solution is the corresponding flag that will be stored in the OCS as a sign of an automatic validation when data is retrieved from the e-signature node. Regarding the format and security features of the flag were presented, obtaining in general positive responses.

Question 1

Would you accept that every citizen record is flagged in the OCS and that this flag is sent in the file the organizers transmit to the National Authorities?

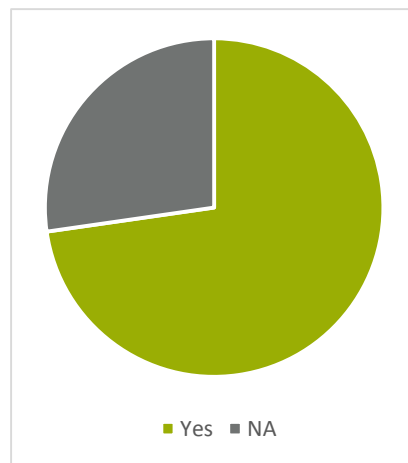


Figure 40: Responses from Member States. Question 1

The responses from Member States regarding this specific point are clearly in favour of the establishment of the flag indicating that the data corresponding to the signatory has already been validated. Member States such as Estonia and Germany have also raised concerns on the fact that the flagging mechanism should be compliant with legislation regarding data protection at European and national level. Implementing a flagging system would not affect the way the data is stored and protected in the OCS. Besides, the flag is created so that it is not possible for organisers to manipulate it in a way that it may be disruptive for the whole ECI process. In short, from a legal point of view, the process of establishing a flag can be carried out when implementing an integration of e-signatures into the Online Collection System.

Question 2

In all of the previous cases, can we still continue with the current process within the Regulation, meaning the organiser sending the file of all their supporters to every national verification authority? (There is a risk that the organisers may put a flag on every record)

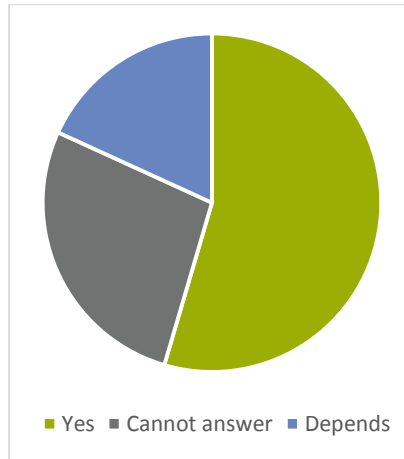


Figure 41: Responses from Member States. Question 2

We can see from the gathered responses that a majority of the Member States consulted would allow the use of the flag in order to account for the previously validated statements of support. The data reflects a common idea shared by most Member States: although statements of support could be considered as automatically validated, verifying authorities would be inclined to continue with the current procedure and receive them to possibly perform additional checks in order to, for example, account for duplicates. Many of the responses that fall in the category “depends”, show a concern for the possibility for organisers to manipulate or tamper the flags and create more “validated” statements of support than they have actually collected.

In this sense, the possibility of including an electronic timestamp when the validation of the data is carried out in the national eID portal was also suggested in the questionnaire, as a way to determine the moment of time in which the statement of support was collected, and to give additional proof of the validity of such data.

Question 3

Could some of the personal data from Annex III be considered as optional?

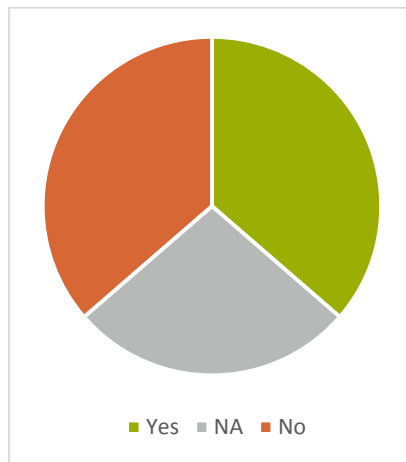


Figure 42: Responses from Member States. Question 3

Regarding this question, the responses are more heterogeneous. More than a third of the Member States consulted were in favour of reducing the data requirements laid down in Annex III. However, at least another third indicates resistance to this possibility, while the rest could not provide an answer at the moment the questionnaire addressed.

Question 4.

Are e-signature certificates issued to a majority of the population?

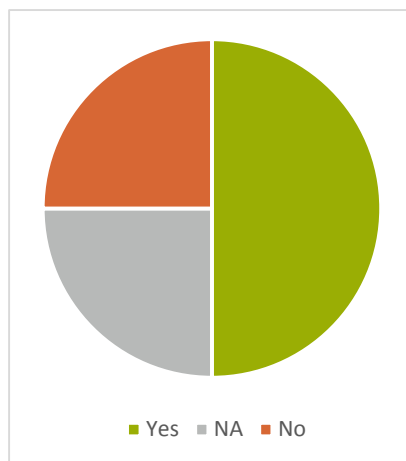


Figure 43: Responses from Member States. Question 4

We can see from the responses gathered that approximately in half of the countries, e-signature certificates have been issued to the majority of population. Countries like Germany, Austria and Estonia responded that e-signature is already issued to all the population over 18 years old. Some Member States who answered negatively have indicated that the number of e-signature certificates issued is larger each year, proof of a growing trend across the EU. However some member states do not issue regularly certificates to their citizens, e.g. France and the Netherlands issue certificates only to representatives of legal persons, whereas other countries do not issue any certificates at all.

To summarise, the responses from Member States show a generally positive opinion towards implementing an integration between the OCS and e-signature means available across Member States. Regarding the possibility of flagging the data retrieved from the e-signature nodes, in general this system is supported by a majority of the consulted sources. And finally, according to the responses, the penetration level of e-signature is already high in several Member States, whereas other sources show a positive trend that proves the suitability of implementing this alternative procedure to submit statements of support. The reluctance of other Member States towards certificates, mainly due to the involved costs, has to be observed.

14.3 BUSINESS ANALYSIS

14.3.1 Ease of use

Citizens

The implementation of this solution offers the signatories a fast and secure alternative for providing their personal data. If the user holds a valid and supported certificate, the e-signature will be created and the statement of support will be submitted in a few clicks. In the event that the solution follows the basic flow described in the use case (see section 14.1.1), the user will not need to insert any other data, leading to a less time-consuming process.

As mentioned in section 14.3.2, the final quantity of data to be inserted depends on the different implementation scenarios proposed. If the solution is derived through the alternative flow, the user has to fill the data requirements after using the e-signature, which results in a more expeditious process.

Finally, it is also important to note that it might be possible that citizens do not have a supported e-signature certificate, depending on its degree of penetration in each Member State (see section 14.3.3), or that the certificate is no longer valid. If these conditions were not met, the submission of a statement of support via e-signature would not be completed.

In essence, compared with the current way of supporting initiatives, the citizens will benefit from a more secure system that reduces the time devoted to submit the statement of support, though a user-friendly process.

Campaign organisers

As far as campaign organisers are concerned, the integration of e-signatures does not significantly impact the way they manage the OCS platform and the data collected.

According to Article 8 of the Regulation, when submitting the statements of support to verifying authorities, organisers have to separate statements of support collected in paper, the ones collected through the OCS and those based on electronic signatures. The proposed changes in the Regulation regarding this aspect were discussed in section 14.2.1. Following this reasoning, no significant impact on the complexity of the OCS can be expected for campaign organisers.

Verifying Authorities

Implementing e-signature will provide a major advantage to Member State's verifying authorities: the validation of the data will be carried out when retrieving them from the certificate, which guarantees its integrity and correctness. Moreover, the identification data contained in the

certificates is very stable and allows to identify the citizen during the entire validity period of a certificate. Notwithstanding, statements of support will be sent to the corresponding verifying authorities following the established procedure, in case they wish to perform further validation checks.

To sum up, e-signature improves the quality of online statements of support, easing the task of validation and the issuing of the certificate (according to the model set out in Annex VI of the Regulation) that accounts for the number of valid statement of support received.

14.3.2 Quantity of data (input)

Citizens

e-signatures contain both data linked to the signed document and to the identity of the signatory. However, as mentioned above, the validation of e-signatures with no additional data will depend on the final technical implementation that this solution follows.

Under the basic flow scenario (see use case, section 14.1.1), statements of support are validated with no additional data, reducing the quantity of data to be inserted manually to zero, beyond the information contained in the certificate. However, within the alternative flow, users still have to type in some of the data, depending on the requirements established by each Member State.

In short, the quantity of data to be inserted by the user generally decreases under solution 2. Depending on how the solution is finally implemented, the user may have to insert some data, although a large part of the data requirements will be largely covered with by the data stored in the certificates.

Campaign organisers

Campaign organisers will be positively affected regarding the data they manage under the current OCS, especially concerning the protection of such data. The integrity and correctness of the data contained in e-signatures enhance security and reduce the legal risks that organisers currently face. This enhanced security features may attract more users, and thus the number of statements of support that they will be able to collect during their campaigning activities.

In addition, implementing this solution will help organisers to better plan and manage their campaign. Since statements of support based on e-signatures provide high confidence in their later validation, they will give organisers a more accurate idea of the number of valid statements collected so far.

Verifying Authorities

The impact for Member State's verifying authorities on the amount of data managed is important, especially if automatic validation is considered. According to the responses obtained from Member State's regarding the flagging system, this solution could be implemented, as they generally show a positive opinion towards this new feature of the OCS (see section 14.2.3).

In this case, the identity of the signatories will not need to be checked again, reducing the number of statements of support that Member States need to validate in order to complete their task. On the other hand, if further verification is required, organisers will follow the procedure described in the Regulation, delivering the statements of support collected in each country to the corresponding verification authority. Under the latter scenario, competent authorities would receive at least the

same number of statements of support as they do under the current procedure, with the added value that the source of the data will be trustworthy and therefore easier to cross-check.

14.3.3 Penetration level / awareness

Citizens

Currently, different operational e-signature creation tools are available across the Member States. Besides, the eIDAS regulation establishes different categories of signature, depending on the Level of Assurance that authorities can have regarding the identity of the signatory. Qualified certificates are issued under supervision of the national competent authorities and comply with the national requirements regarding correctness and integrity of the data. The main benefit of using qualified certificates is that these certificates identify the subscriber and are trusted; the verification of the identity rely on the identity data when these certificates are used.

The level of penetration of this solution can therefore vary largely from one country to another, given the fact that in some countries e-signature is becoming a popular tool, whereas in others its use is not significant yet. As shown in section 14.2.3, Member States have reported a growing number of certificates been issued, and in at least 50% of them, e-signature is available to the majority of the adult population. However some Member States, like France and the Netherlands issue certificates only to representatives of legal personas whereas other don't issue any certificates at all.

In the Member States where a national eID card system has been put in place and smart cards have already been issued to a significant amount of the adult population (Belgium, Germany, Italy, Spain, etc.), the eID cards usually contain certificates allowing the use of e-signature. Accordingly, the impact of this solution is higher in those Member States than in Member States where e-signatures are not widely penetrated.

Nevertheless, it should be noted that if the requirement of qualified certificates were to be extended to all Member States, this solution would exclude Member States in which such certificates are not issued, like the UK, and practically the complete population of Member States, which issue certificates only to representatives of companies, such as France and the Netherlands. On the other hand, if the use of advanced e-signatures is kept, this would not present an issue as advanced e-signatures are available in all Member States.

A special category of certificates is made of certificates that are not held by the subscriber, such as the mobile solutions in Austria and Estonia. These certificates are stored in an HSM (Hardware Security Module) to which physical and logical access is restricted and monitored. Access to the certificate can be granted in various ways, such as access codes sent by SMS or more sophisticated methods. These certificates can only be used for producing signatures.

At this stage of the study, a conclusive assessment of this evaluation criterion is not yet possible. The responses received from Member States to the questionnaire will shed some light on the degree of penetration of the e-signature in each Member State, and the impact that its integration in the OCS might have.

Campaign organisers

The possibility of adding features to the OCS that may make the ECI process more user-friendly and attractive to the general public has a positive impact on organisers. It is easier for them to raise awareness about their campaign and gather a larger number of statements of support.

The reduced legal risks (see section 14.2.1) and enhanced user interface may attract more interested citizens to launch initiatives and bring them to success. However, such effects will be in any case indirect and difficult to assess individually.

Verifying Authorities

Since the e-signature tools selected for integration into the OCS will be the most used in each Member State, it is likely that verifying authorities will trust the information retrieved from those certificates. Hence, the verification task will be facilitated, as the ratio of valid statements of support should be higher.

14.4 TECHNICAL ANALYSIS

The XML structure sent to the signature creation tool must include the name of the initiative as well as other identifier to ensure that when the citizen signs a statement of support for a specific initiative, it is impossible to link the user's data to any other initiative, as mentioned in 5.1.2. The signature creation tool and the XML to be signed must be prepared for the paradigm "what you see is what you sign".

While signature creation tools allow any certificate enabled for signing to create a signature, it would be highly unwise to allow signature-creation with certificates that do not have a key-usage value for it. This, unlike the solution based on authentication with certificates described in solutions 3 and 4, includes certificates stored in an HSM (Hardware Security Module), to which access is granted through username/password schemes, reinforced with mobile phone applications, such as the Austrian and the Estonian mobile solutions.

Generally speaking, such tool also allows the creation of signatures with non-qualified certificates, such as self-issued or employee certificates. Unlike qualified certificates, whose issuing procedure is supervised by a national authority, the user's data of a non-qualified certificate may not always allow to identify unambiguously its owner within the population of the Member State.

14.4.1 Ease of integration

The changes to apply to the OCS, as discussed in 5.1.2, relates to three areas:

- The navigation: These are minor changes which will not present any problems to integrate
- The inclusion of Member State-specific modules: Considering that DSS will be integrated into the OCS, it won't be necessary to implement any MS-specific modules.
- The signing tool should be downloadable from the OCS website and configured for receiving XML data and producing a XAdES signature. Signature tools are complex, and so is their correct configuration. However, no blocking problems are expected with such tool.

Summarising, using DSS will mean an easy integration although the complexity of the signature creation tool may slow down a bit the integration.

14.4.2 Scalability

As mentioned above, the OCS is extended with new custom-built modules, one for each supported Member State, in charge of the following functions:

- The validation of the certificate used for signing
- The extraction of the data from this certificate

These functions present scalability issues in the following cases:

- If any Member State requests the inclusion of more eID means than its national eID, it would lead to the inclusion of an extra module for each new eID, thus presenting a serious scalability problem.

The extraction of the user's data is not straightforward due to the heterogeneous data formats in the available eIDs. As a result, these modules present scalability issues. If the Member States' designated authorities perform this task, it would imply a minor impact on the OCS.

- In case of enlargement of the EU, the inclusion of a new Member State would lead to the inclusion of an extra module, supporting the national eID of this Member State. This process would also apply in case a Member State would leave the EU, causing the need to delete the corresponding module. As such changes in the composition of the EU are not frequent, they should not entail serious scalability problems.

To sum up, the inclusion of Member States' specific modules will cause serious scalability problems as those modules should perform validation of the certificate used for signing or extract the data from this certificate.

14.4.3 Maintainability

The maintainability of the integration of e-signature in the OCS mostly depends on the number of Member State's requests for inclusion of new eIDs enabled for producing e-signatures. Supposing that no new eIDs are included, the maintainability is considered moderate, mainly due to the number of Member States' modules and their complexity. However, if new eIDs are to be included, the maintainability is considered as heavy due to this number of modules and their complexity.

Furthermore, in the following cases, several issues for maintainability can be expected:

- If the Certification Authority's signing certificate for the eIDs or CRLs changes: The OCS will trust a limited set of CAs. Any change in this set will require a change in the configuration of the OCS.
- If the method to find the validation service of a Member State changes: if such method is changed from CRL to OCSP, the Member State's module will need to be adapted to these changes.
- If the format of the data in the national eID changes: the Member State's modules will need to be adapted to this format.

Regarding performance and usage of resources, the integration of e-signatures in the OCS has an impact on the disk and CPU requirements. The increase of requirements on disk space is due to the fact that signed XML structures occupy space in the database: for a signed XML, an estimated size would be around 5kb, while the disk space of user's data may be estimated in 1-5KB. Compared to the current OCS storage, the resulting storage increase for a successful initiative would be 1 Gb, given the size of the new attributes and assuming that 200,000 statements of support (20% of the global threshold) would use this solution.

The validation of the signature included in the XML structure is performed by the OCS, and in case all the statements of support are produced with an eID, the CPU consumption is expected to increase around 70%, compared to the current situation. These estimations are based on performance tests in the STORK project. Considering the same tests, the throughput of a single OCS server can be estimated to be in 50 validations per second, or over 4 million per day, without seriously influencing

the response times. If any performance issue would be found, it could be solved either by using an HSM (Hardware Security Module) for signing, by using multiple servers, or by using both. Many available HSMs have throughputs of over 1000 signatures per second, but these devices are expensive. In most cases, the installation of an HSM is motivated by an increase of the security, not of the performance. Using several servers would be a better option in this case, as it is more economic and offers a linear increase of the performance.

14.4.4 Security

Security on data storage

As far as the current security measures for the OCS meet the ECI Regulation and Commission Implementing Regulation requirements, i.e. the requirements from the Regulation and the requirements of the ECI technical specifications, these measures should also be applied to the new attributes. The signature guarantees the integrity of the XML structure: any change in the contents of the structure would invalidate the signature.

Security on data transmission

The data transmissions between the OCS and the citizen use a secure channel (SSL or TLS), so the confidentiality is guaranteed by the encryption used in this channel. The integrity of the transmitted data is the signature itself: any corruption of it would invalidate it.

Session management

Http is a “stateless” protocol, i.e. all transactions are fully independent of previous transactions. In order to maintain a session, applications use cookies or variables; most Java application servers use the variable JsessionID, whose value determines the thread to which the http request is passed in order to handle it. This variable should be transmitted as a cookie, with the http-only clause, in order to avoid session hijacking.

The vulnerable point is session management is between the reception of the signature and the user’s confirmation of his support. This must be protected with the explained cookie mechanism.

Fraud prevention

The citizen’s agreement is required for producing e-signatures; it is impossible to sign an XML structure with a qualified certificate on behalf of another person. The OCS easily detects copying XML structures: the used certificate would be the same in the copied structure and in the original one.

As qualified certificates are required, the OCS can also verify the citizen’s data against duplicates. As the signed XML contains the name of the initiative, copying this structure to the database of other initiatives is easily detected. In such cases these statements can be rejected.

However, this solution allows EU citizens from non-EU countries to vote.

14.4.5 Maturity

Since the European signature directive (1999/93/EC) and its adoption in the legislation of all EU Member States, electronic signatures have become normal use in applications which require content commitment. The entry into force of the eIDAS Regulation reinforced their legal value and established clear standards that are applicable in all Member States.

According to the research carried out, e-signature certificates are issued to the vast majority of the population of most Member States by qualified trust service providers, and in many countries the complete adult population holds a valid e-signature certificate, (see section 14.2.3 for further discussion). Therefore, the solution is in a mature state that fosters a successful implementation. However, it should be highlighted that some Member States, like France and the Netherlands issue certificates only to representatives of legal personas whereas other don't issue any certificates at all.

14.4.6 Portability

The current implementation of the OCS uses Java as a programming language: the adaptation to be made must also use the Java development platform in order to allow an easy integration. Java is portable to all commonly used operating systems; mostly it does not even require a recompilation. Java source can be used with most current versions of common application servers, like Tomcat, Glassfish, JBoss, WebLogic and WebSphere. However, a solution built on one of the application servers will likely need a porting in order to be used on other application servers too.

The new modules don't use databases but flat files. The main portability issue with flat files is located in the filenames: the directory separator in Windows is backslash (\), while in Unix / Linux platforms this separator is a slash (/). This affects the filenames in configuration files, not the filenames in the Java code, as these are translated at compilation time.

This solution can be used on PCs, tablets, smartphones and any other device supporting Web navigation. However, certificates stored in cryptographic devices will require a reader to be connected to such navigation device, which is not normal practice. The mobile solutions like the Austrian and Estonian ones do not suffer this requirement. Also crypto-cards with the contactless feature, like the German nPA and the new version (3.0) of the Spanish DNIE connect directly to smartphones, and do not require external readers.

14.4.7 Costs / efforts

The efforts required for the inclusion of signed XML structures in the OCS depend on the changes required in the OCS:

- If no new eIDs will be included, an estimation of the required efforts would be 1.5 man-month for each of the 28 modules; in total between 1.5 and 2 man-years.
- If new eIDs will be included, an estimation of the required efforts would be 1.5 man-month for each of these modules; in total around 30 man-months.

15 APPENDIX D – SOLUTION 3: DIRECT INTEGRATION OF EID

15.1 DETAILED DESCRIPTION

A European citizen supports an initiative. To prove his/her identity, he/she presents his/her eID to the OCS website, with the national eID enabled for authentication.

Action ID	Actor	Description
1	Citizen	<p>Support initiative</p> <p>The citizen decides to support an initiative. After some pages where he/she may read all details of the initiative, the button “Support” on the final informative page leads to the OCS</p>
2	OCS	<p>Request data</p> <p>The OCS presents a page where the user is requested to indicate his home country, and depending on this country he/she is requested to fill his personal data. This page also presents a button “Use eID to support”</p> <p>Please note that on this page there is one more button: “Support” which leads to the traditional OCS functionality. There could also be some other buttons, corresponding to other ways to support this initiative. These options are irrelevant in this chapter.</p>
3	Citizen	<p>Click “Use eID to support”</p> <p>The citizen clicks the button “Support with eID”.</p>
4	OCS	<p>Request certificate</p> <p>The OCS establishes SSL / TLS with client authentication, which provokes the browser to request the user to present a certificate. One of the parameters in this establishment is the CAs whose certificates can be accepted.</p>
5	Citizen	<p>Select certificate</p> <p>The user is prompted to select a certificate, and he/she selects an authentication certificate. If the certificate is stored in a cryptographic device, the user will need to introduce the device’s PIN, in order to achieve access to the storage of the card where the private key is kept.</p>
6	OCS	<p>First validation</p> <p>The OCS performs a basic validation on the certificate:</p> <ul style="list-style-type: none"> • If the timestamp “notBefore” is before the system date/time • If the timestamp “notAfter” is after the system date/time • If the certificate has been issued in a European MS (the value of the attribute “C” of the issuer is in the list of EU Member State’s abbreviations: AT, BE, BG, CY, CZ, DE, etc.) • If the issuing CA is present in the Member State’s list of trusted CAs (the certificate is qualified) • If the CA issues certificates to legal persons, the OID of the certificate is checked against a list of permitted OIDs for this CA (the ones corresponding to natural persons) <p>If not all requirements are met, the presented eID is discarded, and</p>

		no data are pre-filled. The same form as from action 2 is presented to the user, with no other data than the previously retrieved data. If the CA allows the validation with OCSP ⁴⁵ , this method is used in activity 7. Else, CRL ⁴⁶ is the method to be used for validation; this is performed in activity 8-10.
7	MS validation	Validate certificate If the validation service is OCSP, this web service checks the certificate on revocation, and replies the status of the certificate to the requesting service.
8	OCS	Request download CRL The OCS requests the CRL to be downloaded from the site indicated by the TSL or by the corresponding attribute in the certificate.
9	MS validation	Send CRL The download request from the OCS is responded by sending the requested file.
10	OCS	Validate certificate The CRL is examined, verifying that the certificate presented by the user is active (not revoked or suspended). This validation requires in the first place the signatory of the CRL: the certificate used for the signature must be the CA's root certificate or issued under the same root certificate of the CA which issued the citizen's certificate. Secondly, the signature is verified: the signature must be valid and produced with a certificate enabled for signing CRLs. Next the scope of the CRL is verified: if a CA certificate is present in the CRL, all certificates signed with this certificate are to be considered revoked. Finally, the list of individually revoked certificates is verified not to include the citizen's certificate.
11	OCS	Validate response The response is validated. If the validation service was OCSP, the signature of this service is validated: its signing certificate must be present in the OCS' trust store.
12	OCS	Extract data The OCS extracts the data from the presented eID. In order to perform this extraction, the specific Member State's modules are invoked. The extracted data are filled into the form in which the user should fill in all his data.
13	OCS	Request confirmation The OCS requests the user to confirm his support to this initiative.
14	Citizen	Confirm support The citizen confirms his support to the initiative by clicking the

		button “Support”.
15	OCS	Store support The OCS stores this statement of support in its database.

Table 39: Description of the actions for the collection of statements of support

15.1.1 Use Case 1: Collection of statements of support

Citizens interested in supporting an initiative will find a user interface that will be slightly modified in order to include a support button for eID and start the process of retrieving personal data from the national eID certificate. The process to be followed is described in the following use case:

Direct integration of eID	
Name	Direct integration of eID and the OCS platform
Description	Connection to Member State’s national eID node in order to retrieve the user’s personal data to submit a statement of support
Actor (Generic)	EU citizen with the right to vote for the European Parliament
Preconditions	<ul style="list-style-type: none"> The user has a valid national eID In case the used eID tool is a smart card, the user has the appropriate hardware (card reader) to use it.
Basic flow	<p><u>Direct integration</u></p> <p>The user:</p> <ol style="list-style-type: none"> 1. Accesses the ECI website 2. Selects a specific initiative to support 3. Clicks on the “Support” button 4. In the data-filling webpage, selects his/her country 5. Selects the “use eID” option 6. If the certificate is stored in a cryptographic device, the user introduces his/her PIN 7. Once the data is retrieved, the user confirms the submission of the statement of support
Exception flow	<ul style="list-style-type: none"> The user is not in possession of a supported national eID solution The certificate is no longer valid, revoked or cannot be read <p><u>Resolution:</u> the statement of support is submitted by typing the data manually into the OCS</p>
Post conditions	The statement of support is submitted.
Devices	<ul style="list-style-type: none"> Computer or portable device⁴⁷ If the eID is stored in a smart card, a card-reader is also required

⁴⁷ Portable devices support soft certificates. Also, mobile ID, like the Austrian and Estonian ones are supported. eIDs stored in cards are generally not supported, unless a reader is connected to this device, or the card counts with connection features, like version 3.0 of the Spanish DNIe, whose RF-ID feature allows connecting with mobile phones.

Software	Supported Internet Browser
Hardware	A card reader is required to access the data if the eID is based on a smart card

Table 40: Use case - direct integration of eID

The scenario described in the basic flow assumes that statements of support will only be validated with the data contained in the eID certificate, without requiring any additional data.

Actors

Abbreviation	Description
Citizen	A European citizen, with the right to vote in elections for the European Parliament, willing to support an initiative
OCS	Online Collection System. A system designed to collect statements of support for initiatives
MS validation	External system used for validation of certificates. The most used method is the publication of a CRL, less popular is OCSP.

Table 41: Actors for collection of statements of support

Activity diagram

The following diagram illustrates the actions and dataflows between the involved parties in the collection phase.

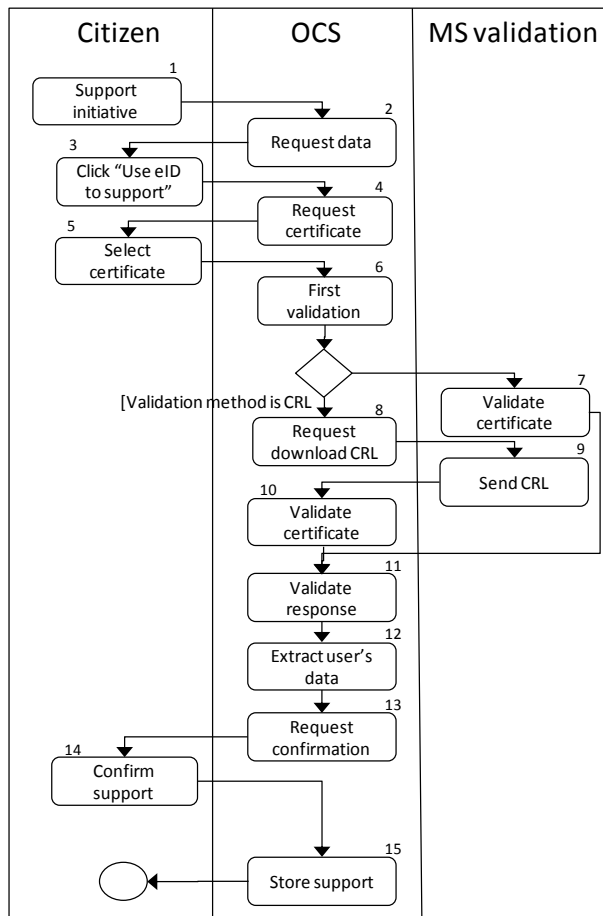


Figure 44: Activity diagram of the collection process

One activity is worth highlighting, the activity 6: **First validation:**

During this activity, the OCS performs a basic validation on the certificate:

- If the timestamp “notBefore” is before the system date/time
- If the timestamp “notAfter” is after the system date/time
- If the certificate has been issued in a European MS (the value of the attribute “C” of the issuer is in the list of EU Member State’s abbreviations: AT, BE, BG, CY, CZ, DE, etc.)
- If the issuing CA is present in the Member State’s list of trusted CAs (the certificate is qualified)
- If the CA issues certificates to legal persons, the OID of the certificate is checked against a list of permitted OIDs for this CA (the ones corresponding to natural persons)

If not all requirements are met, the presented eID is discarded, and no data are pre-filled. The same form as from action 2 is presented to the user, with no other data than the previously retrieved data.

15.2 OVERVIEW OF THE LEGAL FRAMEWORK

The legal analysis carried out for this solution is twofold: First, an ECI Regulation analysis is developed, followed by an overview of the eID AS IS situation across the European Union, based on the responses received to the questionnaires made available to Member States representatives.

15.2.1 Analysis of the ECI Regulation

As mentioned, solution 3 considers a regulatory change regarding ECI. The following analysis focuses on key aspects of the regulation that need to be assessed when attempting to implement this solution, by thoroughly reviewing the content of all the relevant Articles and pointing out possible changes that in order to provide a proper legal support for the presented solution.

The following table provides a review of the ECI regulation, focusing on three main pillars: submission of statements of support (Articles 5 and 6), verification of statements of support (Article 8) and protection of personal data (Article 12):

	Solution 3	Requirements (ECI)	Review
<p>Submission of statements of support</p>	<p>Solution 3 is based on the use of a valid national eID tool that the signatory uses to retrieve his/her personal data from it in order to complete the submission of a statement of support.</p>	<ul style="list-style-type: none"> ○ Art. 5.1(ECI): only forms that comply with Annex III may be used for the collection of statements of support. ○ Art. 5.2 (ECI): statements of support may be collected in paper form or electronically. Statement of support signed with advanced electronic signatures shall be treated in the same way as those submitted in paper form. ○ Art. 6.1(ECI): the OCS shall be certified in accordance with Article 6.3 by the competent authority of the Member State in which the data will be stored. The models for the statement of support forms may be adapted for the purpose of the online collection. ○ Art. 6.2 (ECI): the OCS shall be compliant with the conditions stated in Article 6.4. ○ Art. 6.3 (ECI): the relevant authorities shall issue a certificate (according to the model set out in Annex IV) confirming that the OCS complies with the requirements of Art. 6.4. ○ Art. 6.4 (ECI): the Online collection systems shall have the adequate security and technical features in order to ensure that: <ul style="list-style-type: none"> ○ only natural persons may submit a statement of support; ○ the data provided online are securely collected and stored, in order to ensure, inter alia, that they may not be modified or used for any purpose other than their indicated support of the given citizens' initiative and to protect personal data against accidental or unlawful destruction or accidental loss, alteration or unauthorised disclosure or access; ○ the system can generate statements of support in a form complying with the models set out in Annex III, in order to allow for the verification by the Member States in accordance with Article 8(2). 	<p>This solution is based on the data requirements set out in Annex III in order to retrieve the data stored in the eID, complying with Article 5.1.</p> <p>Since the scope of this solution considers the possibility of a change in Regulation, a specific mention to the use of eID when submitting a statement of support should be taken into consideration.</p> <p>It might be possible that the data stored in any given eID tool does not fully cover the data requirements that each Member State established, but with the data present in the eID, the identity of the signatory can be determined with a high level of assurance. In such case, and compliant with Article 6.1, paragraph 2, the model for creating the statement of support will be modified in order to include only the data present in the eID.</p> <p>The characteristics and features that are required for the OCS to be certified by Member State's competent authorities are laid down in Article 6 of the Regulation.</p> <p>This solution is designed to ensure that only natural persons can complete the process, and the data to be retrieved from the eID will be stored in the same way as when users type in their data manually, complying with the two first conditions in Article 6.4. Only a marker or flag will be added in the database to signal that certain data fields were retrieved from the eID, and can be considered as automatically validated.</p> <p>In order to comply with the last condition of Article 6.4, a modification in Annex III is desired, in order to include the possibility to use eID for the purpose of submitting a statement of support.</p> <p>If the conditions established in Article 6.4 are met, the OCS will be certified by Member State's competent authorities of the country where the OCS is located, as Article 6.3 states.</p>

<p>Verification of statements of support</p>	<p>Once the collection phase of an initiative has come to an end, organisers separate the statements of support collected in paper, and electronically through the OCS, and submit them to Member States.</p> <p>The fact that the data is retrieved from national eID tools could allow those statements of support to be considered as de facto validated. They are still sent in case verifying authorities want to conduct further validity checks and duplicates check with the statements of support collected in paper form.</p> <p>Verifying authorities receive the statement of support and, after verifying the identity of signatories, shall certify the number of valid statements of support presented.</p>	<p>o Art. 8.1 (ECI): organisers shall submit the collected statements of support, in paper or electronic form, to the relevant competent authorities for verification and certification. For that purpose, they shall use the form set out in Annex V, and separate the statement of support collected in paper, from those electronically signed, and those collected through an OCS.</p> <p>Organisers shall submit statements of support to the relevant Member State as follows:</p> <ul style="list-style-type: none"> o To the Member State of residence or of nationality of the signatory, as specified in point 1 of Part C of Annex III, or; o To the Member State that issued the personal identification number or the personal identification document indicated in point 2 of Part C of Annex III. <p>o Art. 8.2 (ECI): The competent authorities shall verify the statements of support received on the basis of appropriate checks, in accordance with national law and practice. On that basis, they shall deliver to the organisers a certificates (according to the model in Annex VI), certifying the number of valid statements of support, for the Member State concerned.</p> <p>For the purpose of the verification of statements of support, the authentication of signatures shall not be required.</p>	<p>If this solution is implemented, the statements of support submitted using eID will be sent online to the competent authorities, in accordance with Article 8.1. The form set out in Annex V will still be followed, separating all kinds of statements of support, with a specific section including the statements of support based on eID.</p> <p>When connecting to each MS node to validate the information, the OCS will obtain a seal or flag that will be stored together with the data. This seal or flag certifies that this data has already been validated. If so, when verifying authorities receive the statements of support to be validated, they can count those as already validated given the fact that they come from trustworthy sources and have already been validated by eID authorities.</p> <p>When implementing this solution, it would be advisable to amend Article 8 in order to include a specific mention about the automatic validation of data coming from eIDs, with a flag/indicator that will account for those statements of support that have been already validated. Besides, the format of the flag that will be created and stored with the data retrieved should be properly defined, preventing a possible tampering of such data or any unlawful use of it.</p> <p>The fact that a special indicator is placed together with the data retrieved from national services is in line with the division of the statements of support that Article 8 mandates when sending them to the competent national authorities.</p> <p>Regarding the Member State to which those statements of support shall be submitted to, the Annex III should be modified by adding a specific criteria for the statements of support submitted via eID. Those should be sent to the country issuing the eID, in case national authorities wish to carry out further validation or checks for duplicates.</p> <p>The rest of statements of support will be sent to the corresponding Member State, according to the criteria of residence/nationality and the personal identification number.</p>
---	--	---	--

<p>Data protection and liabilities</p>	<p>The data retrieved from national eIDs is stored in the OCS, that comply with the security requirements in order to get certified by the Member State where the server is located.</p>	<p>Art. 5.3 (ECI) Signatories shall indicate only the personal data required for the purpose of verification by the Member States.</p> <p>Art.12.1 (ECI): In processing personal data pursuant to this Regulation, the organisers of a citizens' initiative and the competent authorities of the Member State shall comply with Directive 95/46/EC and the national provisions adopted pursuant thereto. This reference to the Directive has to be understood as made to Regulation (EU) 2016/679, which repeals such Directive.</p> <p>Art.12.2 (ECI): The organisers of a citizens' initiative and the competent authorities shall be considered as data controllers, in accordance with the definition provided in Article 4(7) of Regulation 2016/679.</p> <p>Art. 12.3 (ECI): The organisers shall ensure that personal data collected for a given citizen's initiative are not used for any purpose other than their indicated support for that initiative, and shall destroy all statements of support received for that initiative and any copies thereof at the latest one month after submitting that initiative to the Commission or 18 months after the date of registration of the proposed citizens' initiative, whichever is the earlier.</p> <p>Art. 12.4 (ECI): The competent authority shall use the personal data it receives for a given citizens' initiative only for the purpose of verifying the statements of support and shall destroy all statements of support at the latest one month after issuing the certificate.</p> <p>Art. 12.6 (ECI): The organisers shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.</p>	<p>Some eIDs may contain extra information not required for the purpose of submitting a statement of support (e.g. biometric information). In accordance to Article 5.3, this solution will not require citizens to provide any extra information, and only the relevant data for validating the identity of a signatory will be stored in the OCS.</p> <p>The data that will be retrieved from the eID should be protected against unlawful uses, according to Article 12. Once the statements of support are validated and presented to the European Commission, organisers will destroy all of them within one month, or 18 months after the collection phase has finalised, whichever is the earliest (Article 12.3) No change in the way data is managed and destroyed is foreseen for this solution.</p> <p>The OCS will include all the necessary measures to ensure protection of such data (Article 12.4), in order to obtain certification by the Member State's competent authority where the server is located, as stated in Articles 6.1, 6.3 and 6.4.</p> <p>Hence, organisers and verifying authorities will continue to comply with the regulation regarding data protection, and no extra information will be retrieved from eIDs. As a consequence, this solution can be implemented with no change in the Regulation regarding data protection.</p>
---	--	---	--

Table 42: Legal analysis, ECI Regulation - solution 3

Based on this review of the ECI Regulation, it appears that certain aspects of the Regulation require a modification in order to make the proposed integration of eID fit the regulatory framework under which the ECI is currently operating.

Regarding the collection phase, a specific mention to the possibility of using eID to submit a statement of support would be ideal. Accordingly, Annex III would also have to be modified with the purpose of adjusting the personal data requirements of each Member State to the data that could be retrieved from their eID solution in case signatories decide to use this alternative method for submitting their statement of support.

Before the OCS connects to a specific eID validation service, the information is retrieved from its national eID portal and that trustworthy data could thus be considered as automatically validated. For that purpose, a flag is created and added to the validated data in order to give proof of the validation that was carried out automatically when retrieving the data. This major change in the verification process needs to be addressed by the ECI Regulation. Article 8 should thus be amended, adding a mention of the automatic validation when using eID for creating a statement of support.

Although the verification task could be carried out automatically, statements of support are still delivered to verifying authorities in case they want to carry out a second verification or a check for duplicates. Annex III should also be modified in pursuance of the establishment of a new criterion for organisers to know where to send such statements of support. The most logical approach would be to send statements of support created by means of eID to the issuing country of the eID method used, as those are the only ones able to verify the data by checking it against national registries.

Finally, Article 12, which deals with data protection, do not have to be modified, as the data stored is still protected against unlawful uses or losses, as long as the OCS complies with the security requirements stated in Article 6.4.

In light of the information presented, and bearing in mind the possibility of a regulatory change, eID could be implemented into the OCS, requiring only minor changes in the ECI Regulation.

15.2.2 Analysis of Member States responses

The analysis of the situation of eID in the EU Member States is based on the information gathered through desk research as well as on the responses obtained from the questionnaires made available to representatives of each Member State. In total, 12 Member States shared their information:

- Austria
- Belgium
- Czech Republic
- Estonia
- Finland
- Germany
- Greece⁴⁸
- Luxembourg
- Netherlands
- Portugal
- Slovakia
- Spain

⁴⁸The information obtained from Greece was provided by a former representative who is awaiting to be replaced by the new appointed official. Therefore, the data regarding Greece cannot be considered as official.

Key questions regarding the functioning of the ECI process and the current state of eID across the European Union were selected, extracting and processing the information in order to provide useful insights, aiming at assessing the possible roadblocks that this solution might face when implemented.

As mentioned in 15.2.1, an indicator will be kept together with the information received from the corresponding eID node, as a proof of the presence of validated information regarding the signatory that would, in theory, not be checked again. Different alternatives were presented, in order to provide Member States with additional security measures to ensure a lawful and trustworthy implementation of this solution. The possibilities to store only the flag attached to the name of the signatory, to also store all the data retrieved from the eID database, and to include a timestamp were raised, obtaining in general positive responses from the Member States.

Question 1

Would you accept that every citizen record is flagged in the OCS and that this flag is sent in the file the organizers transmit to the National Authorities?

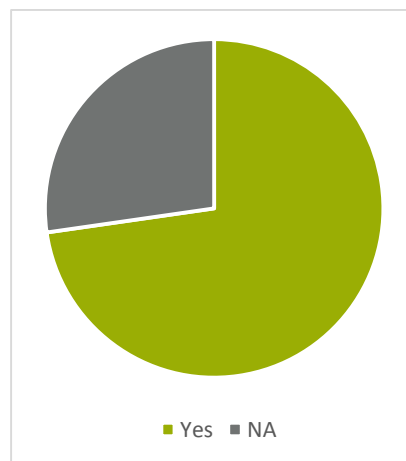


Figure 45: Responses from Member States. Question 1

The responses from Member States regarding this specific point are clearly in favour of the establishment of the flag indicating that the data corresponding to the signatory has already been validated. Member States such as Estonia and Germany have also raised concerns on the fact that the flagging mechanism should be compliant with legislation regarding data protection at European and national level. According to the information presented in section 15.2.1, implementing a flagging system would not affect the way the data is stored and protected in the OCS. Besides, the flag is created so that it is not possible for organisers to manipulate it in a way that it may be disruptive for the whole ECI process. In short, from a feasibility point of view, the process of establishing a flag can be carried out when implementing a direct integration of the eID into the Online Collection System.

Question 2

In the previous case, can we still continue with the current process within the Regulation, meaning the organiser sending the file of all their supporters to every national verification authority? (There is a risk that the organisers may put a flag on every record)

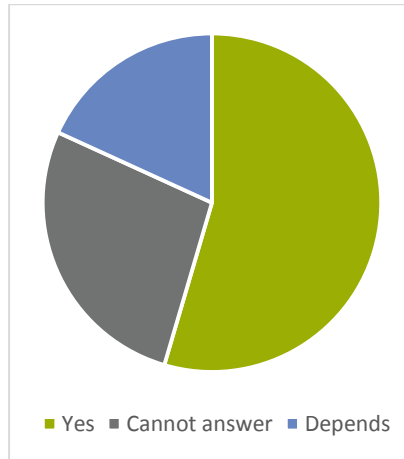


Figure 46: Responses from Member States. Question 2

We can see from the gathered responses that a majority of the Member States consulted would allow the use of the indicator/flag in order to account for the previously validated statements of support. The data reflects a common idea shared by most Member States: although statements of support could be considered as automatically validated, verifying authorities would be inclined to receive them and possibly perform additional checks in order to, for example, account for duplicates. Many of the responses that fall in the category “depends”, show a concern for the possibility for organisers to manipulate or tamper the flags and create more “validated” statements of support than they have actually collected.

As the certificate and the user’s data are stored in the OCS database, possible duplicates are easily detectable.

Question 3

Could some of the personal data from Annex III be considered as optional in the cases where there is a validation by means of an eID?

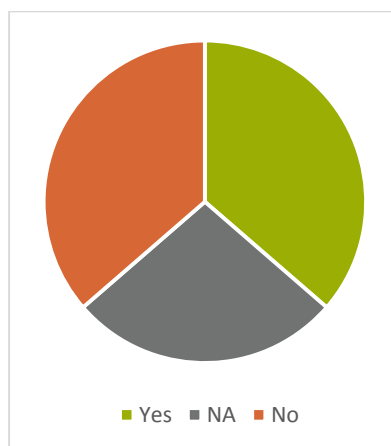


Figure 47: Responses from Member States. Question 3

Regarding this question, the responses are more heterogeneous. More than a third of the Member States consulted were in favour of reducing the data requirements laid down in Annex III. However, at least another third indicates resistance to this possibility, while the rest could not provide an answer at the moment the questionnaire addressed.

This situation reflects a discordant opinion towards the modification of Annex III. Anyhow, this issue may not have a negative effect on the implementation of any eID solution, given the fact that in most of the cases, the information contained in a given eID matches the personal data requirements, and is sufficient to establish the identity of a citizen. Further discussion on this aspect can be found in section 15.3.2.

Question 4

Is eID issued only to natural persons?

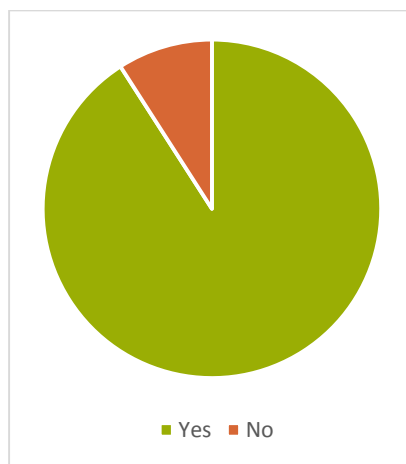


Figure 48: Responses from Member States. Question 4

One of the basic requirements established in the ECI Regulation regarding the right to submit statements of support is to be an EU citizen. The fact that, by implementing this solution, legal persons could also be able to support an initiative is far from trivial, as it could disrupt the whole ECI mechanism. In light of the information presented, it is now clear that this risk will be avoided: only one of the consulted Member States (Spain) is currently issuing eID certificates to legal persons. However, the competent authorities specified that the eIDs issued to legal persons can be differentiated, preventing thus an unlawful use of this alternative method to support an initiative.

Question 5

Is an interactive verification (automatic validation) on the Internet feasible both legally and technically?



Figure 49: Responses from Member States. Question 5

In order to establish a direct integration with eID databases all across the European Union, the user need to authorise the extraction of such sensitive data. For this purpose, an interactive verification of the identity of the citizen whose data is requested seems unavoidable. Regarding this specific question, the Netherlands is the only country that expressed that, by the time this report was written, there is no interactive verification with their eID single access point. In the rest of the Member States, and always according to the responses from the questionnaires, interactive verification is already implemented.

As a summary, the information gathered from Member States can be summarised in two main points:

- In general, Member States share a positive opinion towards an implementation of an eID connection to the OCS. Positive feedback has been received regarding the flagging system and the possibility to consider certain data requirements from Annex III as optional, in case the Regulation was to be modified, enabling validation with the data present on the signatory eID.
- Legal and technical constraints such as being able to distinguish natural and legal persons through the eID solution and having in place an interactive verification that allows for automatic validation of the data can be overcome. This aspect signals the desirability and feasibility of the implementation of this solution from the perspective of the Member State's national legislation point of view.

15.3 BUSINESS ANALYSIS

The business analysis will be conducted by assessing the impact of the proposed solution according to the four following criteria:

1. Ease of use
2. Quantity of data / Input
3. Penetration of the solution/awareness
4. Costs/efforts

Those criteria will be analysed according to each relevant stakeholder involved (citizens, organisers and Member State's verifying authorities).

15.3.1 Ease of use

Citizens

When a citizen accesses the ECI entry point with the purpose of supporting an initiative, the user interface will only be slightly changed in the page where the user is supposed to fill in the data. In the website, a support button for the use of eID will be included. The use case (see section 15.1.1) details all the steps required to complete this process.

Provided that the users hold a valid national eID whose use is supported by the OCS, the process will be smooth and fast, and the personal information will be securely retrieved, completing the submission of the statement of support in a few clicks.

Depending on the national eID solution used by the signatory, he/she might need to use a card reader (which can be included in the computer or as a hardware item connected via USB), and a specific software in order to read the certificate and retrieve the information.

Last but not least, it is also important to note that it might be possible that citizens do not have a supported eID certificate, depending on the degree of penetration of eIDs in each Member State (see section 16.3.3), or that the certificate is no longer valid. If those issues are encountered, the process will display errors and the user will have to type his/her data manually in order to submit a statement of support.

In summary, on condition that the users are in possession of a valid eID tool and the specific hardware that might be required, citizens will benefit from a more secure system and a less time consuming process, as retrieving the data from the eID is faster than typing it in.

Campaign Organisers

Regarding campaign organisers, direct integration of the eID into the OCS will not have a major impact on how they manage the OCS and the collected data. The statements of support submitted by means of eID will be sent to the corresponding Member State's verifying authorities following the procedure detailed in Article 8 of the Regulation, as it is done now. Consequently, no significant impact on complexity is expected for campaign organisers.

Verifying Authorities

As regards Member State's verifying authorities, the implementation of a direct integration of national eIDs add a major advantage. The statement of support submitted using this method would be much easier to verify, as the integrity and correctness the signatory's data is guaranteed by the national eID database.

The connection established from the OCS to the corresponding Member State node is made directly, and the validation of the data is carried out by the eID service provider, therefore not requiring any interaction by the European Commission, that will only be in charge of maintaining the OCS and updating it in case any additional nodes need to be included.

Since the task is going to be done automatically through a connection with each Member State's eID portal, verifying authorities will receive statements of support with a flag signalling the ones already validated. Normally, those would not be further checked, as the source of the data will be trustworthy. Verifying authorities only need to validate statements of support signed in paper or submitted online through the OCS, by entering the data manually.

In addition, if the corresponding authority of any Member State wishes to perform additional checks (flags, duplicates, etc.), the statements of support based on eID will be sent to the corresponding verification authority, following the procedure established in Article 8 of the Regulation.

Therefore, direct integration of eID eases the task of verification by creating an automatic procedure to validate an important portion of the statements of support received.

15.3.2 Quantity of data (input)

Citizens

The successful implementation of the proposed solution should not require inputting any additional data. The quantity of data for this solution could be adjusted and redefined with a change of the Annex III, making sure that the data stored in the national eIDs would be sufficient to support an initiative. Furthermore, the possibility of submitting a statement of support with personal data retrieved from national eIDs would require an additional specific indication of this solution in the Regulation, as mentioned in section 16.2.1.

Verifying authorities should be able to recognise the identity of the signatories from the data retrieved from the eIDs, as this information is normally consistent with the one stored in the national registries. As the Table 6 in section 3.2.4 shows, the two main requirements (date of birth and nationality) can be retrieved from a vast majority of eIDs across the EU. When it comes down to additional data requirements, there are cases where not all the information required by a given Member State can be retrieved by their most popular eID solution.

On the other hand, the responses from the Member States to the questionnaires show that a significant part of Member States are inclined to allow the use of eID to create a statement of support in case the Regulation is changed, and they will adjust the personal requirements in order to verify statements of support with the information retrieved from the national eIDs. Consequently, the quantity of data inserted by the user should be reduced to zero, enabling a user to follow the basic flow described in the use case (see section 15.2.1).

Campaign organisers

Regarding campaign organisers, the amount of data they will manage would not increase in a large quantity, although, collecting statements of support that provide certainty on their later validation will help their purposes. Indeed, as nowadays organisers are recommended to obtain an extra 20% statements of support in order to account for invalid ones⁴⁹, the statements of support based on eIDs would give higher confidence in their latter validation, providing a better idea of the number of valid statements of support collected so far.

In brief, implementing solution three may help organisers internally in their planning and assessment tasks; however, the positive impact on the quantity of data managed by organisers would not be significant.

⁴⁹ Le Gouvernement du Grand-Duché de Luxembourg (2015) Potential Benefits Of Electronic Signatures In The Context Of European Citizen Initiatives.p2

Verifying authorities

As previously analysed, the impact for Member States on the amount of data managed would be positive, given the fact that they would consider statements of support based on eID data as automatically validated.

Those statements of support would thus not necessarily require further validation. This change would lead to a reduction of the number of statements of support that Member States need to validate in order to issue the certificate. However, if verifying authorities still want to, additional post-verification and checks for duplicates can still be carried out (further discussion on the verification process and flagging can be found in section 15.2.1). The certificate is then used by the organisers to submit the initiative to the European Commission.

In short, the implementation of this solution reduces the number of statement of support to be verified, enabling verifying authorities to perform their tasks in a shorter period of time, what leads to an enhancement of the overall performance of the system.

15.3.3 Penetration level /awareness

Citizens

Different eID methods have been deployed across the European Union, at different moments in time. As a consequence, the degree of penetration of this solution is heterogeneous across the Member States. For instance, countries where a national eID card system has been put in place and eID cards have already been issued to a vast majority of the adult population (Belgium, Germany, Italy, Spain, etc.), the impact of this solution will be higher than in Member States where the selected eID solution is more recent or less penetrated.

In addition, the degree of penetration will also depend on other factors such as how many services can be accessed with the eID in each country, and the number of citizens that currently use the eID tool for other purposes (access to public notifications, management of bank accounts, tax declarations, etc.).

Moreover, implementing this solution can have further advantages. Since the ECI tool is operational, the amount of sensitive data to be provided by signatories has been mentioned as one of the main disadvantages of the system⁵⁰. If the direct integration is implemented, the user will not have to introduce much sensitive data into the OCS in order to support an initiative, making the system more attractive and user-friendly. As a consequence, more users could potentially be attracted to the ECI tool, enhancing the overall performance of the system.

⁵⁰ Anglmayer, Irmgard. (2015) The European Citizen's Initiative: the experience of the first three years. European Parliamentary Research Service. p. 10
[http://www.europarl.europa.eu/thinktank/es/document.html?reference=EPRS_IDA\(2015\)536343](http://www.europarl.europa.eu/thinktank/es/document.html?reference=EPRS_IDA(2015)536343)

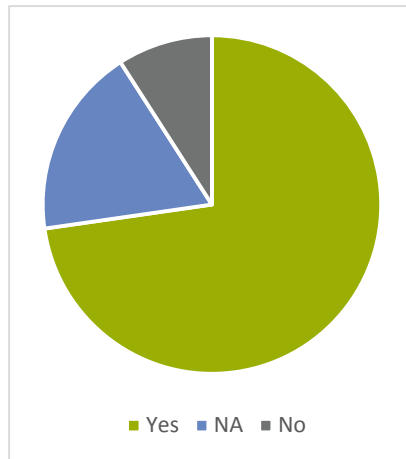
Question 6***Is eID issued to a majority of the population?***

Figure 50: Responses from Member States. Question 6

In order to successfully implement the eID integration solution, it is important to assess the current state of the eID systems deployed in all the Member States. Implementing the direct integration of eID into the OCS at an EU level when a solution is not operational in a given Member State will hinder this solution to achieve its full potential. Fortunately, according to the desk research carried out and the responses obtained from Member States, the penetration of eID in the EU is at a good state of play.

Generally speaking, almost every Member States have implemented, or will soon implement, an eID scheme⁵¹ that will be suitable for integration in the ECI online collection system. However, exceptions can be found in the Netherlands or France (certificates are only issued to representatives of companies). Besides, eIDs have already been issued to the majority of the population in the Member State's consulted. Even where eID is not automatically issued to the adult population (Czech Republic and Greece), national authorities have reported a growing number of users getting access to it.

Campaign Organisers

From the organisers' point of view, the possibility of adding additional features to the OCS that may make the ECI process more user-friendly and attractive to the general public can have a positive impact, as it will help raising awareness about the campaigns and gather a larger number of statements of support.

Regarding data protection, organisers could also benefit from this solution. Currently, organisers are considered as data controllers under Regulation (EU) 2016/679 (repealing Directive 95/46/EC, mentioned in the ECI Regulation) during the collection phase (Article 12, paragraph 2 of the ECI Regulation), being held responsible for any damage they cause (Article 13).

The data retrieved from eID enhances security of the overall system. This improved data security and integrity reduces the legal risks and may attract more concerned citizens to become organisers and campaign for any given cause. However, the effects aforementioned will be in any case indirect, and thus difficult to assess individually.

⁵¹ <https://ec.europa.eu/digital-single-market/en/e-identification>

Verifying Authorities

As the solution selected for integration into the OCS will generally be the one provided or endorsed by the national public authorities, the signatories' information retrieved from their eID corresponds to the official data, meaning that it can be trusted. In such case, the verification task will be easier because data should be identical to the information from the national citizens' registry, leading to a higher ratio of valid statements of support.

15.4 TECHNICAL ANALYSIS

15.4.1 Ease of integration into the OCS

The direct integration of eIDs entails two changes in the Online Collection System: (1) in the navigation and (2) in the inclusion of Member States specific modules:

1. With the direct integration of eID, the navigation in the OCS will need some adaptations such as the inclusion of a button to launch the retrieval of the user's eID and display of the extracted data. These are considered minor changes and will not represent any problem for the integration.
2. The Member States specific modules to be integrated into the OCS are in charge of the validation of the used certificate and the extraction of the user's data. The amount of modules (28) to integrate in the OCS as well as their complexity, lead to a difficult integration.

A limited set of standard methods for validating a certificate is available; the most used ones are based on CRLs (Certificate Revocation Lists, as specified in RFC3280⁵²), while the most modern is called OCSP (Online Certificate Status Protocol)⁵³. Whereas OCSP is a simple protocol based on one type of request and implying one type of answer (the status of the certificate), CRLs are more complex. CRLs may include a scope which needs to be interpreted, and may also be complete or partial (delta). Currently, no other methods are used by the Member States.

Even though the effort of integration is reduced by the mitigation of the problem of integrating 28 modules with the TSL (Trusted Services List) mechanism and the limited number of mechanisms for validation, it still remains high. In order to facilitate the invocation of the correct mechanisms and find the right location (URL) where to find them, the European Commission publishes a "master TSL" (XML format) linking to national TSLs (XML format), which specifies for each qualified CA, the location and method for checking the validity of the certificates.

The wide variety of formats of the citizen's data, in the different certificates, represents a problem. Nonetheless, as these extraction functions are relatively simple functions, these problems are not considered critical, even taking into consideration all national eIDs available for authentication. Considering that citizens are identified by the data in their qualified certificate, this extraction function could not be implemented in the OCS.

As a summary, the integration of this solution is complex due to the 28 specific modules, each of which is moderately complex.

⁵² RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
<https://www.ietf.org/rfc/rfc3280.txt>

⁵³ RFC 6960: X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP

15.4.2 Scalability of direct integration of eID

As mentioned above, the OCS is extended with new custom-built modules, one for each supported Member State, in charge of the following functions:

- The validation of the certificate used for signing
- The extraction of the data from the certificate⁵⁴

These functions present scalability issues in the following cases:

- If any Member State would request the inclusion of more eID means than only its national eID, it would imply the inclusion of an additional module for each new eID, which would represent a serious scalability problem.

The extraction of the data is not straightforward due to the heterogeneous data formats in the available eIDs. If the OCS would not need to perform this extraction because these authorities agree that the citizen is completely identified by his qualified certificate, the extraction would imply a minor impact on the OCS. Besides, this would also present scalability problems with the inclusion of new eIDs.

- In the context of the enlargement of the EU, adding a new Member State would entail the need for inclusion of an extra module per Member State, supporting the national eID. This process would also apply in case a Member State leaves the EU, entailing in this case the need to remove a module. As such changes in the composition of the EU are not frequent, it should not entail serious scalability problems.

15.4.3 Maintainability of direct integration of eID

The maintainability of the direct integration of eID is complex due to the number of specific modules and their dependence on parameters in the certificates, like the OIDs used for natural persons, location of the CRL or OCSP, etc.

15.4.4 Performance and usage of resources

The direct integration of eID has an impact on the required CPU. In case all the statements of support are produced with an eID, the CPU consumption is expected to increase around 70%, based on performance tests performed during the STORK project⁵⁵. Considering these performance tests, a modern server can manage up to 50 receptions of eID per second (80.000 each day), without seriously influencing the response time.

Other changes, such as the navigation, do not have a significant impact on the performance and response time. If any performance issue would be found, it could be solved either by using an HSM (Hardware Security Module) for signing, by using multiple servers, or both. Many available HSMs have throughputs of over 1000 signatures per second. In most cases, the installation of an HSM is motivated by an increase of the security, not of the performance. Using several servers would be a better option in this case, as it would offer a linear increase of the performance.

⁵⁴ Another option would be to develop a module to perform a semantic mapping between the data collected in OCS and the data at national level. However, we believe that building such semantic module with its parameters would be much more complex.

⁵⁵ https://www.eid-stork.eu/index.php?option=com_content&task=view&id=366&Itemid=96

15.4.5 Security

Security on data storage

As far as the current security measures for the OCS meet the EC requirements, no further changes are foreseen for the data stored in the OCS database. These requirements are in the first place those mentioned in Article 6, paragraph 4 of the Regulation, and secondly the ones reflected in the ECI technical specifications. The changes in the contents of the database (inclusion of the used certificate) do not imply more user's data. There are therefore no changes required regarding the privacy of these data.

The normal back-up procedure guarantees the recovery of statements of support in case of accidental loss. This procedure should be verified to include the new columns in the database. In order to detect unlawful destruction or alteration, it would be recommendable to periodically guarantee the contents of the database with a signature produced by the server.

Fraud prevention

Authentication via certificates cannot be produced without the explicit agreement of the subscriber of the certificate. It is thus impossible to authenticate on behalf of other persons. Organisers could copy one row in the database into the same database, changing a minimal set of data, but OCS would easily detect this, as the used certificate in both authentications would be the same. However, a certificate stored in the OCS database for one initiative could easily be copied to another initiative without being detected, allowing for fraud, especially if different initiatives are located on different servers.

The OCS can also verify the citizen's data against duplicate statements of support in case qualified certificates are used. But no protection against duplicates is in place if the citizen uses different certificates of the same country, or uses certificates from different countries.

Security of data transmissions

The data transmissions between the OCS and the citizen use a secure channel (SSL or TLS), so the confidentiality is guaranteed by the encryption used in this channel. The integrity of the certificate is achieved with the included signature of the CA.

Currently, the transmission of the statements of support from the organisers to the Member States follows a different procedure for each Member State. It is proposed to use a homogeneous procedure consisting of:

- For paper-based statements of support, these are scanned into one file.
- All statements of support – both the electronic ones and the scanned paper ones – are compacted in a ZIP format, protected with encryption.
- Considering the file-size, the compacted file is stored on a file-server available on the Internet, and not sent directly to the Member States.
- The link to the file, together with the decryption key is sent by email to the corresponding Member State's verification authority. This email, including its attachment, is protected for integrity by the organiser's signature. The confidentiality is protected with encryption using the recipient's public key.

The transmission of the verification certificate from the Member State's verification authority is sent by email using the same security measures protecting its integrity and confidentiality.

Session management

Http is a "stateless" protocol, meaning that all transactions are fully independent from the previous ones. In order to maintain a session, applications use cookies or variables; most Java application servers use the variable JsessionID, whose value determines the thread to which the http request is passed in order to handle it. This variable should be transmitted as a cookie, with the http-only clause, in order to avoid session hijacking.

15.4.6 Maturity

Since the European e-signature directive (1999/93/EC), and its adoption in the legislation of all EU Member States, authentication with eIDs, especially certificates, became common in different kind of applications. In most Member States, the eID has been implemented and a major part of the population, starting from a certain age, owns a citizen card, containing certificates. However, in some Member States such as France and the Netherlands hardly any certificates are issued to the citizens.

15.4.7 Portability

The current implementation of the OCS is based on the programming language Java. By consequence, the required modifications must also be developed via the Java development platform, in order to ease the integration. Java is portable to all commonly used operating systems; mostly it does not even require a recompilation. Java source can be used with most current versions of common application servers, like Tomcat, Glassfish, JBoss, WebLogic and WebSphere. However, a solution built on one of the application servers will most likely need a porting in order to be used on other application servers too.

The new modules do not use databases, just flat files. The main portability issue with flat files is located in the filenames: the directory separator in Windows is backslash (\), while in Unix / Linux platforms this separator is a slash (/). This affects the filenames in configuration files, not the filenames in the Java code, as these are translated at compilation time.

This solution can be used on PCs, tablets and smartphones. However, this portability may be limited by the need to connect readers for the eID containing devices: smartcards are not commonly used with tablets and smartphones. Such readers are not required with portable solutions as the Austrian and Estonian mobile solutions, nor are they required with contactless cards, like the German nPA and the new version of the Spanish DNle.

15.4.8 Costs / efforts

Considering the problems of validation of the certificates, the efforts required for the inclusion of the direct integration of eID in the OCS depend on the changes required in the OCS:

- If the OCS performs the checks on validity and the extraction of the citizen's data, and no new eID is included, an estimation of the required efforts would be 1.5 man-months for each of the 28 modules; in total between 1.5 and 2 man-years.
- If the OCS performs the checks on validity and the extraction of the citizen's data, and new eID is included, a first rough estimation of the required efforts would be 1.5 man-months for each of these modules; in total more than 2 man-years.

16 APPENDIX E – SOLUTION 4: INTEGRATION WITH THE EIDAS FRAMEWORK

16.1 DETAILED DESCRIPTION

A European citizen would like to support an initiative. To prove his/her identity, he/she presents his/her eID through the eIDAS platform to the OCS website.

Action ID	Actor	Description
1	Citizen	<p>Support initiative</p> <p>The citizen decides to support an initiative. After going through the details of the initiative, the button “Support” on the final informative page leads to the OCS.</p>
2	OCS	<p>Request data</p> <p>The OCS presents a page where the user is requested to indicate his/her home country, and depending on this country, requested to fill his/her personal data.</p> <p>Please note that on this page there is also a button: “Support” which leads to the traditional OCS functionality. This option is irrelevant in this chapter.</p>
3	Citizen	<p>Click “Use eID to support” button</p> <p>The citizen clicks on the button “Support with eID”.</p>
4	OMS eIDAS node	<p>Validate Requester</p> <p>The EC eIDAS node verifies that the requester is authorised to launch the request towards its node by checking that the certificate of the CA which issued the requester’s certificate is present in the EC node’s trust store.</p> <p>The token is also checked on a syntax point of view</p>
5	Browser	<p>Redirect</p> <p>The browser redirects the user to the Member State of the citizen, the one he/she indicated.</p>
6	CMS eIDAS node	<p>Validate Requester</p> <p>The MS eIDAS node verifies that the requester is authorised to launch the request towards its node by checking that the certificate of the CA which issued the requester’s certificate is present in the MS node’s trust store.</p> <p>The token is also checked on a syntax point of view.</p> <p>Please note that activities 7 to 12 are specific to each Member State.</p>
7	Browser	<p>Redirect</p> <p>The browser redirects the user to the IDP of the Member State.</p>
8	CMS IDP	<p>Request eID</p>

		The IDP requests the user to present his eID. This may be any type of eID, which complies with the requirements, especially the Level of Authentication, set by the OCS.
9	Citizen	Introduce eID The citizen introduces his national eID. This may be a certificate, but it could also be any other eID which is nationally used.
10	MS IDP	Validate eID The national IDP validates the used eID
11	Browser	Redirect The browser redirects the user to the eIDAS node of the Member State of the citizen.
12	CMS eIDAS node	Validate response The eIDAS node of the Member State validates the response. Please note that with this activity the specific interaction ends
13	Browser	Redirect The browser redirects the user to the eIDAS node of the EC.
14	OMS eIDAS node	Validate response The eIDAS node of the EC validates the response. This entails the validation of the signing certificate of the sender: the issuer of this certificate must be present in the trust store of the EC eIDAS node.
15	Browser	Redirect The browser redirects the user to the OCS.
16	OCS	Validate response The OCS validates the response. This entails the validation of the signing certificate of the sender of this certificate must be present in the trust store of the OCS.
17	OCS	Extract the user's data The OCS extracts the user's data from the SAML token, and fills them in the statement of support form.
18	OCS	Request confirmation The OCS presents the statement of support form with all user's data, and requests the user to confirm his support to this initiative
19	Citizen	Confirm support The citizen confirms his/her support to the initiative by clicking the button "Support".
20	OCS	Store support The OCS stores this statement of support in its database.

Table 43 : Description of the actions for the collection of statements of support

16.1.1 Use Case 1: Collection of statements of support

In this context, the solution will be based on a connection between the OCS and the eIDAS framework, retrieving data once the citizen has used his/her eID certificate. The process to submit a statement of support using this solution will be very similar to solution 3, direct integration of eID (see section 6.1.1). The following use case describes all the steps to be followed in order to complete the submission:

Indirect integration of eID (eIDAS)	
Name	Indirect integration of eID and the OCS through the eIDAS network
Description	Connection to Member State's eIDAS node in order to retrieve the user's personal data in order to submit a statement of support
Actor (Generic)	EU citizen with the right to vote for the EP
Preconditions	<ul style="list-style-type: none"> • The user is interested in supporting an initiative through the OCS • The user is willing to use his/her national eID in order to submit the statement of support • The user has a valid national eID
Basic flow	<p><u>eIDAS integration</u></p> <p>The user:</p> <ol style="list-style-type: none"> 1. Accesses the ECI website 2. Selects a specific initiative to support 3. Clicks on the "Support" button 4. In the data-filling webpage, selects his/her country 5. Selects "use eID" 6. is redirected to his/her home country eID website 7. Selects his/her eID 8. Unlocks this eID with the password or PIN 9. (is redirected back to OCS) 10. The data is retrieved, the user confirms the submission of the statement of support
Exception flow	<ul style="list-style-type: none"> • The user is not in possession of a supported national eID solution • The certificate is no longer valid, revoked or cannot be read <p><u>Resolution:</u> statements of support are submitted by typing data into the OCS</p>
Post conditions	<ul style="list-style-type: none"> • The statement of support of an initiative is submitted.
Devices	<ul style="list-style-type: none"> • Computer or portable device⁵⁶ • If the eID is stored in a smart card, also a card-reader is required

⁵⁶ The support of portable devices depends on the facilities of each MS' notified eID. In general, soft certificates and (reinforced) username / password schemes are supported. As far as certificates are stored in user-held devices (cards, USB sticks, etc.), readers for such devices should be connected to the portable device.

Software	Supported Internet Browser
Hardware	In case the eID is based on a smart-card, a card reader will be required to access the data.

Table 44: Use case - indirect integration of eID connecting to eIDAS network

Provided the user holds a valid national eID whose use is supported by his national eIDAS node, the process, similarly to what is described in solution 2, is completed in a few clicks. Connecting to the eIDAS network only adds one additional step, as the user is redirected to his/her eID issuing Member State website in order to access the data and complete the transition. Nonetheless, the differences in the back-end and the architecture of this solution are significant.

Actors

The actors mentioned in the activity diagram in the next section are described as follows:

Actor	Description
Citizen	Natural persons forming a citizen's committee responsible for the preparation of a citizens' initiative and its submission to the Commission
Browser	A software tool designed to navigate web pages on the Internet
OCS	The Online Collection System. A system designed to collect statements of support for initiatives, often hosted by the EC
OMS eIDAS node	The eIDAS node located in the Member State where also the OCS is located, the connection point for the EC to the eIDAS platform
CMS eIDAS node	The eIDAS node located at the Member State of the citizen's eID
MS IDP	The identity provider of the Member State, in charge of issuing the eIDs, also in charge of its verification

Table 45: Actors for the collection of statements of support

Activity diagram

The following diagram illustrates the actions and dataflows between the involved parties in the collection phase.

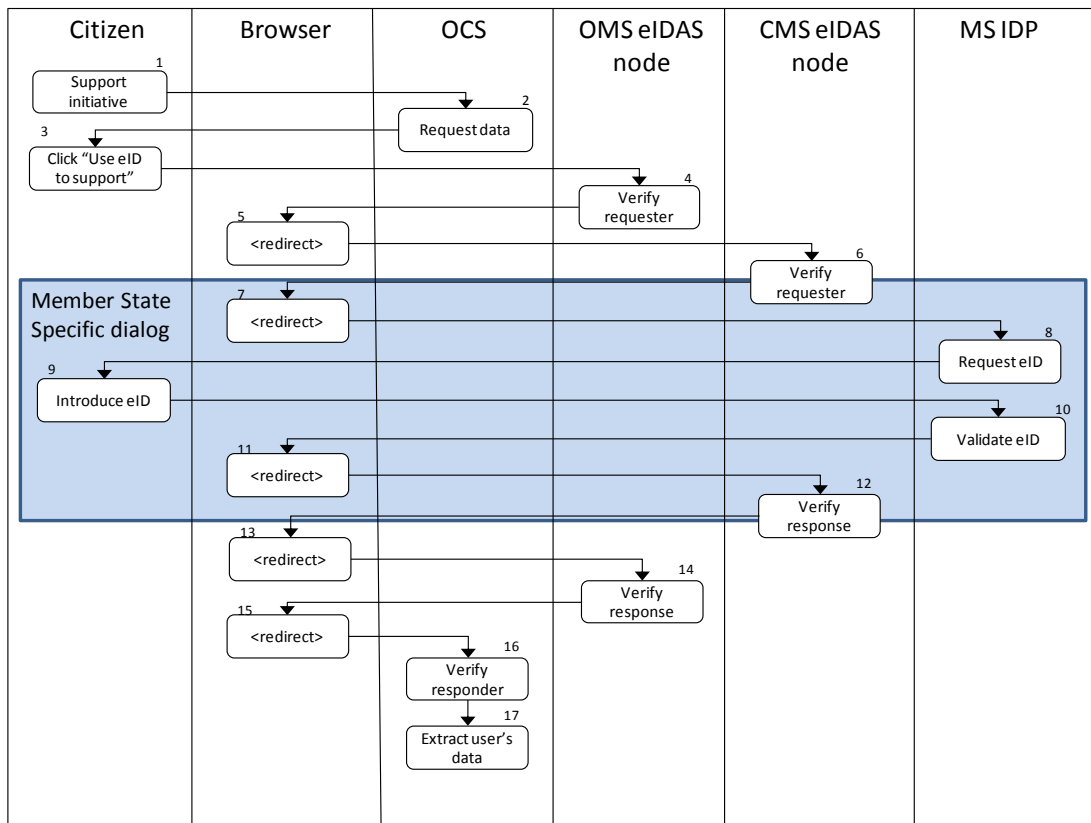


Figure 51: Activity diagram of the collection process - part 1⁵⁷

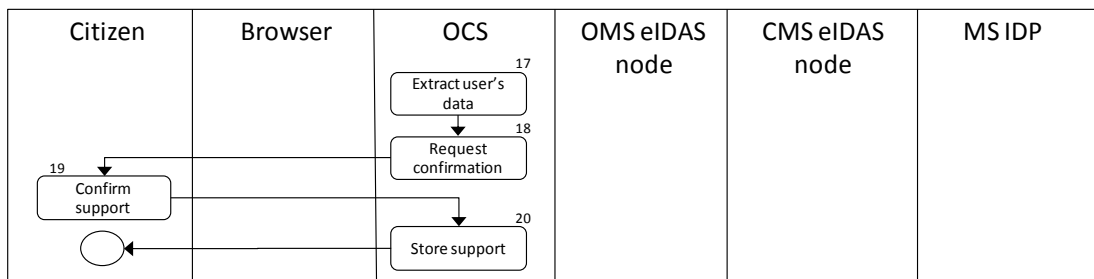


Figure 52: Activity diagram of the collection process - part 2

16.2 OVERVIEW OF THE LEGAL FRAMEWORK

16.2.1 Analysis of the ECI Regulation

Following the same approach, the legal analysis will depart from a thorough review of the current regulatory framework, focusing on three main areas:

- Submission of statements of support (Articles 5 and 6)
- Verification of statements of support (Article 8)
- Data protection requirements (Articles 5, 6 and 12)

⁵⁷ Please note that the dialog in the first diagram, with the blue background is specific to each member state. The dialog in this diagram represents the typical interactions in case a certificate is used for authentication.

	Solution 4	Requirements (ECI)	Review
<p>Submission of statements of support</p>	<p>Solution 4 is based on a valid national eID tool that the signatory use to retrieve his personal data, connecting to the national eID portal through the eIDAS network in order to complete the submission of a statement of support.</p>	<ul style="list-style-type: none"> ○ Art. 5.1 (ECI): only forms complying with Annex III may be used for the collection of statements of support. ○ Art. 5.2 (ECI): statements of support may be collected in paper form or electronically. Statement of support signed with advanced electronic signatures shall be treated in the same way as those submitted in paper form. ○ Art. 6.1 (ECI): the OCS shall be certified in accordance with Article 6.3 by the competent authority of the Member State in which the data will be stored. The models for the statement of support forms may be adapted for the purpose of the online collection. ○ Art. 6.2 (ECI): The OCS shall be compliant with the conditions stated in Article 6.4. ○ Art. 6.3 (ECI): the relevant authorities shall issue a certificate (according to the model set out in Annex IV) confirming that the OCS complies with the requirements of Article 6.4. ○ Art. 6.4 (ECI): Online collection systems shall have the adequate security and technical features in order to ensure that: <ul style="list-style-type: none"> ○ only natural persons may submit a statement of support; ○ the data provided online are securely collected and stored, in order to ensure, inter alia, that they may not be modified or used for any other purpose than their indicated support of the given citizens' initiative and to protect personal data against accidental or unlawful destruction or accidental loss, alteration or unauthorised disclosure or access; ○ the system can generate statements of support in a form complying with the models set out in Annex III, in order to allow for the verification by the Member States in accordance with Article 8(2). 	<p>This solution is based on the data requirements set out in Annex III in order to retrieve the data stored in the eID, complying with Article 5.1.</p> <p>Since the scope of this solution considers the possibility of a change in Regulation, a specific mention to the use of eID when submitting a statement of support should be taken into consideration. Given the fact that solution 3 foresees the access to the eIDAS network for the request of information to identify signatories, a specific mention to the eIDAS Regulation would be advisable to provide the proper legal basis for its implementation.</p> <p>It might be possible that the data shared in eIDAS by many MS does not fully cover the data requirements that each one of them has established, but according to the eIDAS Regulation, both the Minimum Data Set and the Optional Data Set are sufficient to establish the identity of any natural person. Thus, the identity of the signatory can be determined with a high level of assurance. In such case, and compliant with Article 6.1, paragraph 2, the model for creating the statement of support is modified in order to include only the data shared by the corresponding MS within the eIDAS framework.</p> <p>The characteristics and features that are required for the OCS to be certified by Member State's competent authorities are laid down in Article 6 of the Regulation.</p> <p>This solution is designed to ensure that only natural persons can complete the process, and the data to be retrieved from the eID via the eIDAS node will be stored in the same way as when users type in their data manually, complying with the two first conditions in Article 6.4. Only a marker of flag will be added in the database to signal that certain data fields were retrieved from the eID, and can therefore be considered as automatically validated.</p> <p>In order to comply with the last condition of Article 6.4, a modification in Annex III is desired, in order to include de possibility to use eID for the purpose of submitting a statement of support, accepting the submission of a statement of support with the data shared by the corresponding Member State through the eIDAS network.</p> <p>If the conditions established in Article 6.4 are met, the OCS will be certified by Member State's competent authorities of the country where the OCS is located, as Article 6.3 states.</p>

<p>Verification of statements of support</p>	<p>Once the collection phase of an initiative has come to an end, organisers separate the statements of support collected in paper, and electronically through the OCS, and submit them to the Member States.</p> <p>The fact that the data is retrieved from national eID tools could provide that those statements of support are considered as de facto validated. Nonetheless, they are still sent in case verifying authorities want to do further validity checks and duplicates check with statements of support collected in paper.</p> <p>Verifying authorities receive the statement of support, and after verifying the identity of signatories, they shall certify the number of valid statements of support presented.</p>	<p>o Art. 8.1 (ECI): organisers shall submit the collected statements of support, in paper or electronic form, to the relevant competent authorities for verification and certification. For that purpose, they shall use the form set out in Annex V, and separate the statements of support collected in paper, from those electronically signed, and those collected through an OCS.</p> <p>Organisers shall submit statements of support to the relevant Member State as follows:</p> <ul style="list-style-type: none"> o To the Member State of residence or of nationality of the signatory, as specified in point 1 of Part C of Annex III, or o To the Member State that issued the personal identification number or the personal identification document indicated in point 2 of Part C of Annex III. <p>o Art. 8.2 (ECI): The competent authorities shall verify the statements of support received on the basis of appropriate checks, in accordance with national law and practice. On that basis they shall deliver to the organisers a certificates (according to the model in Annex VI), certifying the number of valid statements of support, for the Member State concerned.</p> <p>For the purpose of the verification of statements of support, the authentication of signatures shall not be required.</p>	<p>If this solution is implemented, statements of support submitted using eID are sent online to the competent authorities, in accordance with Article 8.1. The form set out in Annex V is still followed, separating all kinds of statement of support, with a specific section including the statements of support based on the data retrieved from eIDAS.</p> <p>When connecting to the eIDAS node to retrieve the information, the OCS obtains a seal or flag that is stored together with the data. This indicator certifies that this data has already been validated. If so, when verifying authorities received the statements of support to be validated, they can count those as already validated given the fact that they come from trustworthy sources and have been already validated by eID authorities.</p> <p>When implementing this solution, it would be advisable to modify Article 8 in order to include a specific mention about the automatic validation of data through eIDAS. Besides, the format of the flag/or seal that is created and stored with the data retrieved should be properly defined, preventing a possible tampering of such data or any unlawful use of it.</p> <p>Regarding the Member State to which those statements of support shall be submitted to, the Annex III should be modified by adding a specific criteria for the statements of support submitted via eID. Those statement of support should be sent to the country issuing the eID, in case national authorities wish to carry out further validation or check for duplicates.</p> <p>The rest of statements of support are sent to the corresponding Member State, according to the criteria of residence/nationality and the personal identification number issuing Member State.</p>
<p>Data protection and liabilities</p>	<p>The data retrieved from national eIDs are stored in the OCS, that will comply with the security requirements in order to get certified by the Member State where the server is located.</p>	<p>Art. 5.3 (ECI): Signatories shall indicate only the personal data required for the purpose of verification by the Member States.</p> <p>Art.12.1 (ECI): In processing personal data pursuant to this Regulation, the organisers of a citizens' initiative and the competent authorities of the Member State shall comply with Directive 95/46/EC and the national provisions adopted pursuant thereto. This reference to the Directive has to be understood as made to Regulation (EU) 2016/679, which repeals such Directive.</p> <p>Art.12.2 (ECI): The organisers of a citizens' initiative and the</p>	<p>Some eIDs may contain extra information not required for the purpose of submitting a statement of support (e.g. biometric information). In accordance to Article 5.3, this solution will not require citizens to provide any extra information and only the relevant data for validating the identity of a signatory will be stored in the OCS.</p> <p>Besides, the eIDAS Regulation only foresees sharing the two data sets mentioned above (Minimum and Optional), so additional data to the one requested by Member State is in use for the purpose of supporting an initiative.</p>

		<p>competent authorities shall be considered as data controllers, in accordance with the definition provided in Art. 4(7) of Regulation 2016/679.</p> <p>Art. 12.3 (ECI): The organisers shall ensure that personal data collected for a given citizen’s initiative are not used for any other purpose than their indicated support for that initiative, and shall destroy all statements of support received for that initiative and any copies thereof at the latest one month after submitting that initiative to the Commission or 18 months after the date of registration of the proposed citizens’ initiative, whichever is the earlier.</p> <p>Art. 12.4 (ECI): The competent authority shall use the personal data it receives for a given citizens’ initiative only for the purpose of verifying the statements of support, and shall destroy all statements of support at the latest one month after issuing the certificate.</p> <p>Art. 12.6 (ECI): The organisers shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.</p>	<p>The data that is retrieved from the eIDs should be protected against unlawful uses, according to Article 12. Once the statements of support are validated and presented to the European Commission, organisers will destroy all of them within one month, or 18 months after the collection phase has finalised, whichever is the earliest (Article 12. 3). No change in the way data is managed and destroyed is foreseen for this solution.</p> <p>The OCS will include all the necessary measures to ensure protection of such data, (Article 12.4) in order to obtain certification by the Member State’s competent authority where the server is located, as stated in Articles 6.1, 6.3 and 6.4.</p> <p>Hence, organisers and verifying authorities will continue to comply with the regulation regarding data protection, and no extra information will be retrieved from eIDs. As a consequence, this solution can be implemented with no change in the Regulation regarding data protection.</p>
--	--	---	--

Table 46: Legal analysis, ECI Regulation - solution 4

According to the review presented above, some aspects of the ECI Regulation would require a modification in order to make the proposed integration with eIDAS to be clearly binding within the regulatory framework that governs the ECI process.

Regarding the collection phase, a specific mention to the possibility to use eID and connect to the national databases through eIDAS in order to submit a statement of support would be suitable. Accordingly, a modification in Annex III is desirable in order to establish that statements of support will only require the data shared by Member States through eIDAS to be successfully validated, if signatories decide to follow this alternative method of submission.

When the OCS connects to the eIDAS node, the information is retrieved from its national eID portal. The information contained in such certificates, which is sufficient to establish the identity of a citizen according to eIDAS Regulation (Article 8), could be considered as automatically validated. For that purpose, a flag will be created and added to the validated data, in order to give proof of the validation that was carried out automatically when retrieving the data. As mentioned in the legal analysis for solution 3 (see section 15.2.1), a modification of Article 8 would be desirable, establishing the automatic validation of such data as an alternative procedure for the creation of statements of support.

The procedure described for solution 3 is also applicable for the eIDAS connection, as statements of support are sent for verification to the corresponding national authority regardless of the flag placed next to the data that proves automatic verification. Moreover, a modification of Annex III is also to be considered, in order to further establish that the statements of support containing eID data shall be sent to the Member State where the eID was issued.

Regarding data protection (Article 12), the analysis is analogous to the one presented in solution 3: there is no modification in the procedure to store the data. Moreover, protection against loss, interference or unlawful use of the OCS is still compliant with the security requirement established in Article 6.4. Hence, no regulatory change is required on this aspect when implementing this solution.

In consideration of the analysis carried out, and the possibility of a regulatory change, the integration of the eIDAS network and the OCS is a feasible option that would require minor changes in the ECI Regulation

16.2.2 Analysis of the eIDAS Regulation

	Solution 4	Requirements (eIDAS)	Review
<p>Scope</p>	<p>Solution 4 is based on the use of a valid national eID tool that the signatory will use to retrieve his personal data from it, connecting to the national eID portal through the eIDAS network in order to complete the submission of a statement of support.</p>	<p>Art. 1: With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:</p> <p>(a) lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;</p> <p>(b) lays down rules for trust services, in particular for electronic transactions; and</p> <p>(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication</p> <p>Art. 2: This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union.</p> <p>This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.</p> <p>This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.</p>	<p>Article 1 states the main purposes of eIDAS. Specifically, the first and second items in this Article are relevant to the ECI process.</p> <p>Firstly, in order to implement a connection with eIDAS, it is important to establish clear rules and conditions to achieve interoperability among all the Member States, so eID solutions across the Union can be trusted and successfully connected to the OCS.</p> <p>Secondly, trust services play a main role in electronic identification and in the authentication and retrieval of data required in this solution, in order to establish a connection system that becomes a reliable source for verifying authorities so they can consider statements of support as automatically validated.</p> <p>Regarding Article 2, solution 3 clearly falls within the eIDAS scope, as it will be implemented only within the European Union and will establish a connection with trust service providers that are notified and compliant with eIDAS Regulation.</p> <p>Integrating eID solutions into the OCS via the eIDAS network would not result in a closed system determined by national regulations, but the ECI Regulation at EU level. Therefore, eIDAS Regulation is directly applicable to solution 3.</p>

<p>Internal market principle</p>	<p>The OCS will request the data from signatories to the corresponding national eID databases.</p>	<p>Art 4:</p> <ol style="list-style-type: none"> 1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation. 2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market 	<p>Given the fact that, once this solution is implemented, it will be compliant with eIDAS Regulation, the OCS will be fully integrated into the Digital Single Market, and will be able to make request for specific data to the corresponding service providers (national eID databases)</p>
<p>Data protection</p>		<p>Art. 5:</p> <ol style="list-style-type: none"> 1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC. 2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited. 	<p>Data that is input, retrieved and stored in the ECI context has to be protected according to this Regulation. As analysed in section 17.2.1, Article 12 of the ECI Regulation establishes a set of security features that the OCS should have in order to ensure only lawful use of personal data. Therefore, given that such conditions will be met (see section 8.4.5), implementing this solution will be in line with both the ECI and the eIDAS Regulation.</p>
<p>Assurance level</p>		<p>Art.8:</p> <ol style="list-style-type: none"> 2. The assurance levels low, substantial and high shall meet respectively the following criteria: <p>(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;</p> <p>(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity</p> 	<p>In order to establish a reliable eID connection that is able to provide trustworthy data, the eID solutions will need to be consistent with the substantial or high level of assurance. Normally, since the eID tools that will be proposed for integration are based on a national eID scheme, they will be part of that Member State’s trusted list, and therefore be catalogued as substantial or high.</p> <p>According to the research carried out (see Table 3), the majority of Member States already have deployed eID means that provide at least a substantial level of assurance. Thus, once the data has been retrieved and stored with the flag in the OCS, verifying authorities, might not need to perform additional checks in order to establish the identity of the signatory. In any case, and as previously mentioned, statements of support will be delivered to them in case they wish to carry out further validation tasks.</p>

Table 47: Legal analysis, eIDAS Regulation - solution 4

16.2.3 Analysis of Member States responses

Together with the general eID responses analysed for solution 3 (see section 15.2.2), the analysis of solution 3 is complemented with specific questions related to the current state of eIDAS and what information would Member States be willing to share, in order to provide a clear view of the AS IS situation of eIDAS across the European Union.

Question 1

Can you extract nationality from the eIDAS Data set? If not, could nationality be part of the shared data?

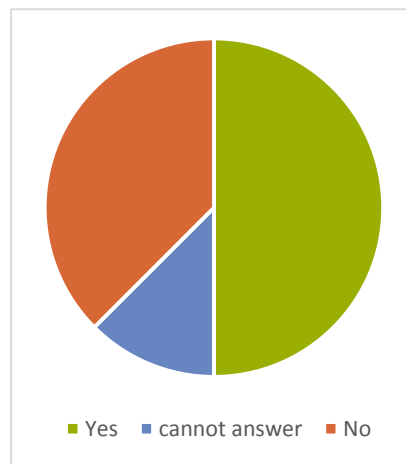


Figure 53: Responses from Member States. Question 7

Given the developing and production state that the Member States' eIDAS nodes is currently facing, information regarding the set of data that each country would be willing to share through eIDAS is scarce and scattered. Thus, the possibility of having the nationality as part of the data shared by eIDAS is of key importance for the implementation of this solution, given the fact that nationality is one of the primary requirements for a citizen to support an initiative within the ECI framework.

The responses obtained prove that there is no common ground regarding among Member States on the nationality being shared for this purpose, although half of the countries show a positive opinion towards this possibility. At the moment this report was written, some of the consulted countries (Greece and Czech Republic) could not provide a definitive answer to this specific question. Countries such as Estonia and Spain have also pointed out that nationality could be extracted from the Unique Identifier number, and therefore sharing nationality would not be needed.

Question 2

Would the eIDAS Unique Identifier be enough for the verification of a statement of support? What other data might be needed?

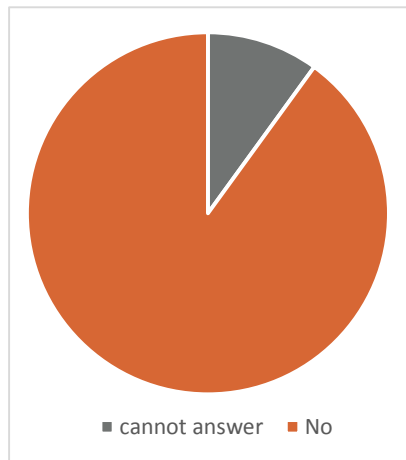


Figure 54: Responses from Member States. Question 8

The Unique Identifier is another main point to assess when analysing a possible integration of eIDAS into the ECI process. This attribute is certainly key when aiming at establishing the identity of the signatory, as it is individually linked to him/her and it remains unchanged through time. When asked about the possibility to only use this single attribute to verify the identity of the citizen that supports an initiative, Member States were generally against it, although a significant number of them (Austria, Belgium, Spain, Germany among others) pointed out that the Minimum Set of Data would be sufficient to establish the identity of a citizen and thus to validate the statements of support. Further discussion regarding this issue can be found in section 16.3.2)

Question 3

Will your national eIDAS implementation make “place of birth” and “residence address” available to other MS?

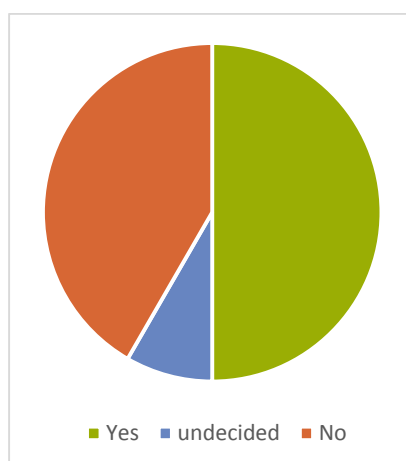


Figure 55: Responses from Member States. Question 9

The question 9 relates to the Optional Set of Data that, depending on the decision of Member States to share it, may provide information (place of birth and residence) required by some countries to

validate the statements of support. The responses were in majority in favour of sharing those relevant pieces of data, although countries such as, Belgium, Spain or Portugal have given a conditional positive response, pending previous authorisation of the citizen himself or of the national agency of data protection. Consequently, taking into consideration their previous responses, almost all Member States who stated they would only require the Minimum Set of Data to validate a statement of support, are not favourable to the possibility of sharing the Place of Birth and Residence, as they consider those data as not necessary to establish the identity of a citizen, with the data retrieved via eIDAS.

In summary, besides the analysis of legal framework of eID integration, the analysis of the specific responses regarding eIDAS shows a general positive attitude from Member States towards its implementation. In particular, the responses show that Member States would be able to establish the identity of the signatories (nationals or residing in their country) with only the Minimum Data Set. Also, the possibilities to derive some other data (i.e. nationality) from the Unique Identifier should also be taken into account.

As Member States are currently immersed in the eIDAS production phase, the analysis shows a lack of consensus regarding the amount of data to be shared through eIDAS, as some countries could not provide a definitive answer at the moment. Nevertheless, the fact that the Minimum Data Set would be sufficient to create a statement of support and establish the identity of a citizen is a positive sign that opens up the possibility of implementing an integration of eID via eIDAS in a majority of the Member States.

16.3 BUSINESS ANALYSIS

16.3.1 Ease of use

Citizens

Considering the ease of use, the differences between Solution 3 (direct integration of eID) and solution 4 (Indirect Integration via eIDAS) are mainly technical, the analysis of this evaluation criterion is comparable to the one carried out for solution 3 (see section 15.3.1). In this case, the process will still be easy to access and complete, as the redirection to the home country eID website before retrieving the data is expected to have very limited impact on the user experience.

Campaign Organisers

As mentioned, integrating eID into the OCS will not have a major change in the way campaign organisers manage the platform and the collected data. Therefore, the fact that the data is retrieved directly or via eIDAS does not make a difference for organisers.

According to what was described in sections 16.2.1 and 16.2.3, no impact on the complexity is expected for campaign organisers once the OCS has integrated this new functionality, as the procedure for sending the statements of support to Member States' verifying authorities (Article 8 of the Regulation) will remain unchanged.

Verifying Authorities

Verifying authorities will receive statements of support with signatories' data coming from trusted sources. As integrating eIDAS and the ECI online platform improves the quality of online statements of support and eases the task of validation, statements of support submitted using this solution can be considered as automatically validated. This automatic validation is made possible thanks to the

system of flags that can be added to the information coming from those trusted sources. This interactive verification will not, however, interfere with the current procedure of sending the statements of support to Member States' verifying authorities, which will still receive them, giving them the possibility to perform additional checks.

16.3.2 Quantity of data (input)

Citizens

Commission implementing Regulation (EU) 2015/1501 only specifies as a Minimum Data Set (Article 11), that all Member States are obliged to comply with when sharing data in eID transactions. This data set includes:

- The current first and last name
- The date of birth
- The unique identifier⁵⁸

Additionally, an optional dataset is defined, including other attributes that may also be required in order to validate the identity of an EU citizen. Those attributes are:

- The first name(s) and family name(s) at birth
- The place of birth
- The current address
- The gender

When implementing this solution, agreements among Member State will need to be reached. Especially, consensus is required regarding which sets of data they will share with each other for the purpose of supporting European Citizens' Initiatives.

Question 8(2):

Would you require only the Minimum Data Set to be sent to the OCS for the purpose of submitting a statement of support?

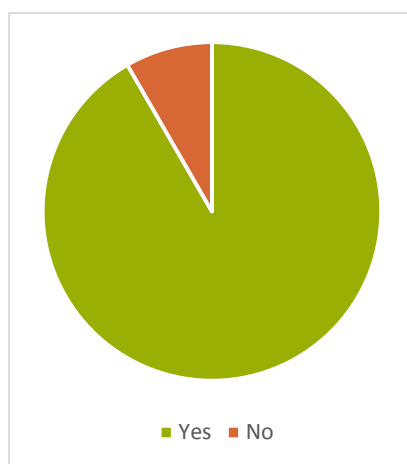


Figure 56: Responses from Member States. Question 8(2)

⁵⁸ According to the Annex of Commission Implementing Regulation (EU) 2015/1501, the unique identifier "is constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time."

After extracting and analysing in depth the collected responses, the analysis can conclude that the vast majority of the Member States consulted are able to establish the identity of the citizens with the Minimum Set of Data. Only Czech Republic pointed out that some extra information (Place of birth, nationality, ID document number, and type of document) is required in addition to the Minimum Set of Data.

Following the responses given by Member State's representatives, solution 4 departs from the assumption that statements of support containing the Minimum Set of Data, established in the eIDAS Regulation, are automatically validated as verifying authorities are able to establish the identity of the signatories. Consequently, the quantity of data to be inserted by the user is reduced to zero.

Campaign Organisers

As stated in section 15.3.2, the effect on organisers will not be significant, as the quantity of data they manage will not be directly affected by the implementation of this solution.

Verifying Authorities

As mentioned in section 15.3.2, the impact for the verifying authorities is positive. The only difference between the two solutions presented in this report being how the connection to the eID database is established.

Once the information has been retrieved and stored in the OCS with the flag indicating validation, the verification task can be considered as automatically carried out, and the corresponding authorities only have to issue the certificate once all the statements of support have been received.

16.3.3 Penetration level /awareness

Citizens

Since the tool used to retrieve the signatory's personal data is the national eID, the analysis regarding the penetration of this solution is comparable to the one carried out in solution 2 (see section 15.3.3). Besides, eIDAS also provides supports to any type of eID, including (reinforced) username / password schemes, so the penetration level is significantly higher than the direct integration of eID.

In addition, connection to eIDAS presents specific challenges, as most eIDAS nodes are still in preproduction mode and therefore not fully operational yet. According to the eIDAS Regulation, by 18 September 2018, mutual recognition of eIDs is mandatory. Although countries such as The Netherlands, Germany and Austria have already successfully connected their eID nodes⁵⁹, the full potential of this solution will not be a reality until all nodes are totally interoperable.

Campaign Organisers

The impact for organisers regarding this evaluation criteria is equivalent to the one analysed for the direct integration of eID into the OCS. For further discussion, please see section 15.3.3.

⁵⁹ Filis, Thomas (2017). *Key Milestone Reached! First Cross Border Connections Between (technically compliant) eIDAS Nodes in Production*. Retrieved from: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Key+Milestone+Reached%21+First+Cross+Border+Connections+Between+%28technically++compliant%29+eIDAS+Nodes+in+Production>

Verifying Authorities

The impact for organisers regarding this evaluation criteria is equivalent to the one analysed for the direct integration of eID into the OCS. For further discussion, please see section 15.3.3.

16.4 TECHNICAL ANALYSIS

16.4.1 Ease of integration

The changes to apply to the OCS, as discussed in 7.1.2 are located in two areas:

1. In the navigation: minor changes that will not present any problems to integrate.
2. With the inclusion of the eIDAS connection module: In principle, the integration of the eIDAS connection module entails the filling into its API of the attribute name / value pairs (normally the requests have empty attribute values), which are transformed by this module to the SAML request according to the eIDAS specifications. The response is disassembled by this connection module into the same name / value pairs. The complex logic of supporting and validating the user's eID and extracting the user's data is delegated to the Member State's eIDAS nodes.

16.4.2 Scalability

As mentioned above, the Online Collection System is extended with the standard module for connecting eIDAS, in charge of the following functions:

- The assembly and sending of the authentication requests to the eIDAS node of the Member State where the OCS is located
- The reception of the responses and their disassembly

Following the recommendations of the IDABC workgroup (2004) for a scalable and maintainable systems-architecture⁶⁰, the STORK project (2008-2011) extended their recommended centralised architecture with the support for the decentralised model⁶¹. This architecture, with minor changes, is still in place in the eIDAS specifications and implementation.

Thus, these functions present no scalability issues: new eIDs or modifications in their configuration only affect the corresponding Member State eIDAS node, while the inclusion of additional Member State in eIDAS would only affect the eIDAS node of the Member State where the OCS is located.

16.4.3 Maintainability

As indicated in previous sections, the eIDAS platform has been designed to be maintainable. Thus, the inclusion of the eIDAS connection module does not represent any maintainability issue. The only changes that might affect this module would be the inclusion of new attributes (e.g. nationality). If these are relevant to the OCS, it would require a change in the configuration of the eIDAS connection module, in order to be able to request and receive these attributes. Such a change would also entail a minor change in the OCS, to store this attribute in the OCS database.

⁶⁰ European Interoperability Framework for pan-European eGovernment Services: <http://ec.europa.eu/idabc/en/document/7641/6014.html>

⁶¹ D4.3 Updated Report on eID Process Flows: https://www.eid-stork.eu/index.php?option=com_content&task=view&id=366&Itemid=96

16.4.4 Performance and usage of resources

This solution affects the required resources in two matters:

- The disk usage
- The CPU

The increase of requirements on disk space is due to the fact that the responses from the eIDAS node occupy space in the database: such a message has an estimated size of around 10Kb. The increase of disk occupation for a successful initiative, supposing that one quarter of the 1.000.000 statements of support would use this solution, would be 2.5 Gb.

The validation of the signature included in the eIDAS message is performed by the eIDAS connection module in the OCS, causing an increase of the CPU consumption of around 70%, based on the performance tests performed during the STORK project⁶². Based on the same tests, the throughput of a simple, non- high availability server, is estimated to 50 authentications per second, or over 4 million per day.

16.4.5 Security

Security on data storage

If the current security measures for the OCS meet the EC requirements, these measures should also be applied to the new columns in the database, especially to the eIDAS message received from the EC eIDAS node. These EC requirements are in the first place those mentioned in Article 6, paragraph 4 of the Regulation, and secondly the ones reflected in the ECI technical specifications. No further changes are foreseen for the data stored in the OCS database. The message itself contains a signature, which guarantees its integrity.

The normal back-up procedure guarantees the recovery of statements of support in case of accidental loss. This procedure should be verified to include the new columns in the database. In order to detect unlawful destruction or alteration, it would be recommendable to periodically guarantee the contents of the database with a signature produced by the server.

The changes in the contents of the database (inclusion of the used certificate) do not imply more user's data. There are therefore no changes required regarding the privacy of these data.

Fraud prevention

Secondly, as authentication responses cannot be produced without the participation of the owner of the eID, it is impossible to authenticate on behalf of other natural persons with an eID of a substantial or high level of assurance. Copying authentication responses is easily detected by the OCS: the responses in the two rows in the database would be the same. Furthermore, the responses include a time-stamp, which makes it easy to detect such copies. The citizen's data can also be verified against duplicates by the OCS.

However, this solution does not offer checks against copying statements of support from one OCS database to the database of another initiative. It could nonetheless be detected, especially by

⁶² https://www.eid-stork.eu/index.php?option=com_content&task=view&id=366&Itemid=96

validating the time-stamp in the responses, but it would entail cross-initiative validations, which are only feasible if all initiatives are located on the same server.

In addition, fraud prevention issues could be raised regarding the Unique Person Identifier attribute in the eIDAS specifications. The Person Identifier's prefix indicates the country where the eID has been issued, but this country may be different from the nationality of the person. If the nationality is not stored in the OCS, some citizens have the possibility to vote twice: once in the Member State of residence and once in the Member State of his/her nationality. Moreover, citizens from outside the EU without the right to vote for the EP would have the possibility support initiatives.

Security of data transmissions

As the data transmissions between the OCS and the citizen use a secure channel (SSL or TLS), the confidentiality is guaranteed by the encryption used in this channel. The integrity of the transmission is guaranteed by the signature on the eIDAS SAML token.

Currently, the transmission of the statements of support from the organisers to the Member States follows a different procedure for each Member State. This study proposes using a homogeneous procedure, which includes measure to protect the integrity and confidentiality of the transmissions of data during the verification phase

Session management

Http is a "stateless" protocol, i.e. all transactions are fully independent from previous transactions. In order to maintain a session, applications use cookies or variables; most Java application servers use the variable JsessionID, whose value determines the thread to which the http request is passed in order to handle it. This variable should be transmitted as a cookie, with the http-only clause, in order to avoid session hijacking. This cookie is very relevant in the link between the session in which the SAML token is received and the confirmation of support by the user.

16.4.6 Maturity

The eIDAS Regulation and the corresponding platform were established in 2014. This platform has therefore not been thoroughly tested in real life environment, and it may be expected that some errors will be found during the integration of solution 4 into the OCS.

At the moment of writing of this document only one eID has been pre-notified (by Germany). Several Member States foresee pre-notifying this year, which increases the expectations of maturity for the near future. However, the platform cannot currently be considered as mature.

16.4.7 Portability

The current implementation of the OCS uses Java as a programming language, as well as the module for connecting to the eIDAS platform. By consequence, the required modifications must also be developed via the Java development platform, in order to ease the integration. Java is portable to all commonly used operating systems; mostly it does not even require a recompilation. Java source can be used with most current versions of common application servers, like Tomcat, Glassfish, JBoss, WebLogic and WebSphere. However, a solution built on one of the application servers will likely need a porting in order to be used on other application servers too.

The new modules don't use databases but flat files. The main portability issue with flat files is located in the filenames: the directory separator in Windows is backslash (\), while in Unix / Linux platforms

this separator is a slash (/). This affects the filenames in configuration files, not the filenames in the Java code, as these are translated at the moment of the compilation.

This solution can be used on PCs, tablets, smartphones or any other device which supports browsing the Web. As far as eIDs are stored in user-held cryptographic devices, corresponding readers should be connected to the navigation-device; this is not common for tablets and smartphones. Such problem does not apply to the Austrian and Estonian mobile solution; neither is it applicable to eIDs stored in contactless crypto-cards, like the German nPA and the new version of the Spanish DNIE.

16.4.8 Costs / efforts

The efforts required for connecting with the eIDAS platform are moderate. As indicated in 7.4, the main expected problem is that this solution has not been tested thoroughly in real life environment, most probably leading to unfound errors. The detection of errors and their correction will require efforts and will especially increase the time frame to achieve a fully operational integration of eIDAS into the OCS. The efforts required for the integration of eIDAS into the OCS are estimated in 4 man-months

17 APPENDIX F – SOLUTION 5: PREFILLING USER’S DATA WITH EU LOGIN

17.1 DETAILED DESCRIPTION

17.1.1 Use Case 1: Collection of statements of support

The table below describes the process and steps to be followed when using the EU Login solution.

EU Login	
Name	Prefilling of a statement of support via EU Login
Description	Connection to the EU Login account to retrieve some of the user’s personal data to ease the submission of a statement of support
Actor (Generic)	EU citizen with the right to vote for the EP
Preconditions	The user has an EU Login account
Basic flow	<p><u>EU Login</u></p> <p>The user:</p> <ol style="list-style-type: none"> 1. Accesses the ECI website 2. Selects a specific initiative to support 3. Clicks on the “Support” button 4. In the data-filling webpage, selects his/her country 5. Selects the option to pre-fill data via EU Login⁶³ 6. Authenticates in the EU Login website 7. The data is retrieved. The user completes the missing data and, if necessary, adapts some of the pre-filled data 8. Confirms the submission of the statement of support
Post conditions	The statement of support of an initiative is submitted
Devices	Computer
Software	Supported Internet browser

Table 48: Use case - EU Login

General description

A European citizen wishes to support an initiative by means of an e-signature. To prove the citizen’s entitlement to support this initiative, she/he presents his national eID.

Actors

Abbreviation	Description
--------------	-------------

⁶³ EU Login is limited to serving authentication and corresponding data to EC applications. Currently the OCS, even if it is hosted at the EC premises is not considered as an EC application.

Citizen	A European citizen, with the right to vote in elections for the European Parliament, wishing to support an initiative
Browser	A software tool designed to navigate web pages on the Internet
OCS	Online Collection System. A system designed to collect statements of support for initiatives
EU Login	The European Commission Login system, formerly EC Authentication Service (ECAS), that aims at providing access to every online service provided by the EU, with one single account.

Table 49: Actors for collection of statements of support

Activity diagram

The following diagram illustrates the actions and dataflows between the involved parties in the collection phase.

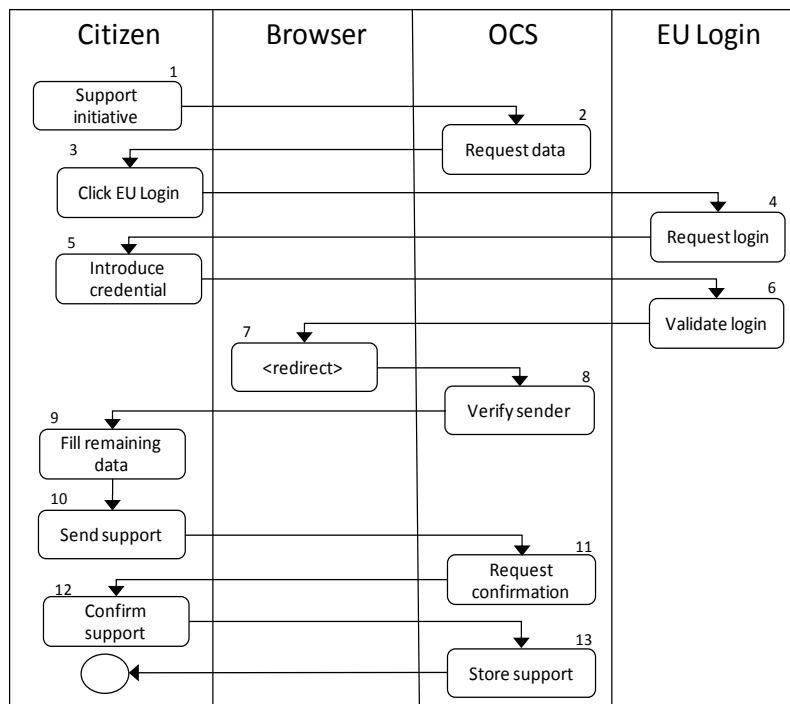


Figure 57: Activity diagram of the collection process

The activities in this diagram are generally self-explaining.

17.2 BUSINESS ANALYSIS

Integration of social networks into the OCS mainly has an effect on one of the stakeholders involved in the ECI: citizens. As this complement will not change how the statements of support are collected or verified, the impact on organisers and Member State’s verifying authorities is not considered to be significant. Consequently, the analysis will only focus on the impact for citizens on each evaluation criterion.

17.2.1 Ease of use

Regarding the user interface, this solution does not present significant differences. However, depending on the data stored, the time devoted to complete the submission, and thus the ease of use of the solution, is different.

Moreover, two-factor authentication methods are becoming popular security features that provide higher degree of certainty on the identity of the user that attempts to gain access to any online service. EU Login provides this method as a way to guarantee only lawful access to their accounts. In this case, the traditional username and password authentication is combined with a code sent to the user's mobile phone. However, this feature can be disabled by the user, and its activation cannot be detected by the receptor of the user's data. In addition, the lawful access to the accounts depends if there is an authentication procedure in place when acquiring phone numbers.

It is also important to consider that this pre-filling options offers the possibility to remove the CAPTCHA, one of the main sources of criticism towards the OCS⁶⁴.

From a usability point of view, the EU Login solution only has a minor impact on the ECI website. A button for the use of EU Login is added on the page where the user has to enter his/her data. The use case described in the introduction (see section 8.1.1) details all the steps required to complete the process.

The data stored in external EU Login accounts is very limited. Therefore, although the signatory will find a user-friendly procedure, the time devoted to complete the submission of the statement of support will increase as he/she introduces the remaining data. Further discussion on the quantity of data included in the EU Login external account can be found in section 17.2.2.

17.2.2 Quantity of data (input)

The EU Login accounts store very little personal data of the users due to privacy and security reasons. Currently, external accounts only store the full name of the user and his/her email. Internal accounts (owned by people professionally involved with the European Commission) store additional information relevant to the ECI requirements, such as date of birth, place of birth and nationality.

However, this type of EU Login accounts is only provided to a very limited range of the population and therefore are not representative of the main use that this complementing tool offers. Consequently, regular citizens who hold a valid external EU Login account have to input manually the rest of the personal data requirements.

17.2.3 Penetration level / awareness

Given the fact that the creation of EU Login as an integrating access point for all the EU services is relatively new, it is not yet used by a significant percentage of the EU population. Besides, only internal accounts have a substantial amount of data to be retrieved when supporting an initiative. The number of accounts validated can be considered as minimal, as it is mainly restricted to EU officials and other internal workers.

⁶⁴ Anglmayer, Irmgard. (2015) The European Citizen's Initiative: the experience of the first three years. European Parliamentary Research Service.
[http://www.europarl.europa.eu/thinktank/es/document.html?reference=EPRS_IDA\(2015\)536343](http://www.europarl.europa.eu/thinktank/es/document.html?reference=EPRS_IDA(2015)536343). P 10

Therefore, the penetration of this complementary solution is not expected to be high, as the EU Login account is still in an early stage of growth.

17.3 TECHNICAL ANALYSIS

17.3.1 Ease of integration

The changes to apply to the OCS relate to three areas:

- The navigation: These are minor changes, which will not present any problems to integrate.
- The inclusion of the EU Login module: The integration of the EU Login requires a simple call to the API with no parameters, and the result is a call from this system, returning attribute name / value pairs. It has been designed for easy integration and has been tested in numerous EC applications. Important integration issues are not expected.

17.3.2 Scalability

As mentioned, the OCS is extended with the EU Login module, in charge of the following functions:

- Composing and sending the authentication request to the EU Login system
- Receiving the response and extracting the data from this response.

These functions do not present any scalability issues: new types of eIDs can be included without affecting the integration in the OCS.

17.3.3 Maintainability

The EU Login module, once integrated in the OCS, is not expected to suffer changes over time, neither for the specifications of their APIs, nor for the supported data. No maintenance on these integrations is therefore expected.

17.3.4 Performance and usage of resources

These solutions impact on the required resources regarding the CPU usage. If 20% of the statements of support would use the feature of EU Login, the validation of the signature included in the response from the EU Login would cause an increase of the CPU consumption of around 14%, based on performance tests in the STORK project. Based on the same tests, the total amount of authentication transactions is estimated in around 50 per second, which is equivalent to over 4 million per day.

17.3.5 Security

This integration is designed to facilitate the filling of the support form of the OCS. As such, no changes in the security performances are anticipated. The only noticeable improvement is the possibility to remove the captcha feature for the users who would choose to integrate with EU Login.

Compared with the current situation, this solution offers no additional guarantees against citizens voting more than once, on behalf of other people, nor against EU residents from non-EU countries supporting initiatives.

17.3.6 Maturity

EU Login, the successor of ECAS, has been launched in production several months ago by DG DIGIT and it is now widely in use, so this solution is to be considered mature.

17.3.7 Portability

This tool is accessible on multiple platforms as it is implemented as web applications. No issues are expected.

17.3.8 Costs / efforts

The little complexity of the EU Login module and its API motivate the efforts required for the inclusion of these modules into the OCS to be estimated as low. Additionally, the large experience of integration of these solutions into applications of the EC and other organisations motivate even more the confidence in a smooth integration.

The efforts required to include EU Login into the OCS involve changes in the navigation and inclusion of the EU Login and Facebook Login modules. They are estimated around 3 man-months.

18 APPENDIX G – SOLUTION 6: PREFILLING USER’S DATA WITH FACEBOOK

18.1 DETAILED DESCRIPTION

18.1.1 Use Case 1: Collection of statements of support

The following table describes the process and steps to be followed when using the Facebook solution:

Facebook	
Name	Prefilling of a statement of support via Facebook
Description	Connection to the Facebook account to retrieve some of the user’s personal data to ease the submission of a statement of support
Actor (Generic)	EU citizen with the right to vote for the EP
Preconditions	The user has a Facebook account
Basic flow	<p>Facebook</p> <p>The user:</p> <ol style="list-style-type: none"> 1. Accesses the ECI website 2. Selects a specific initiative to support 3. Clicks on the “Support” button 4. In the data-filling webpage, selects his/her country 5. Selects the option to prefill data by using the personal data of the Facebook user⁶⁵ 6. The data is retrieved. The user completes the missing data and, if necessary, adapts some of the pre-filled data 7. Confirms the submission of the statement of support
Post conditions	The statement of support of an initiative is submitted
Devices	Computer
Software	Supported Internet browser

Table 50: Use case - Facebook

General description

A European citizen wishes to support an initiative by means of an e-signature. To prove the citizen’s entitlement to support this initiative, she/he presents his national eID.

Actors

⁶⁵ This solution could be leveraged to "social networks" in general. In particular, using the OAuth protocol family for integration opens up possibilities for many social networks all over the world, thus increasing what is called "Penetration" in the document

Abbreviation	Description
Citizen	A European citizen, with the right to vote in elections for the European Parliament, wishing to support an initiative
Browser	A software tool designed to navigate web pages on the Internet
OCS	Online Collection System. A system designed to collect statements of support for initiatives
Facebook	One of the most widespread social networks, which can be used as a complementary tool for prefilling some data of the statement of support based on the user’s data stored by this system.

Table 51: Actors for collection of statements of support

Activity diagram

The following diagram illustrates the actions and dataflows between the involved parties in the collection phase.

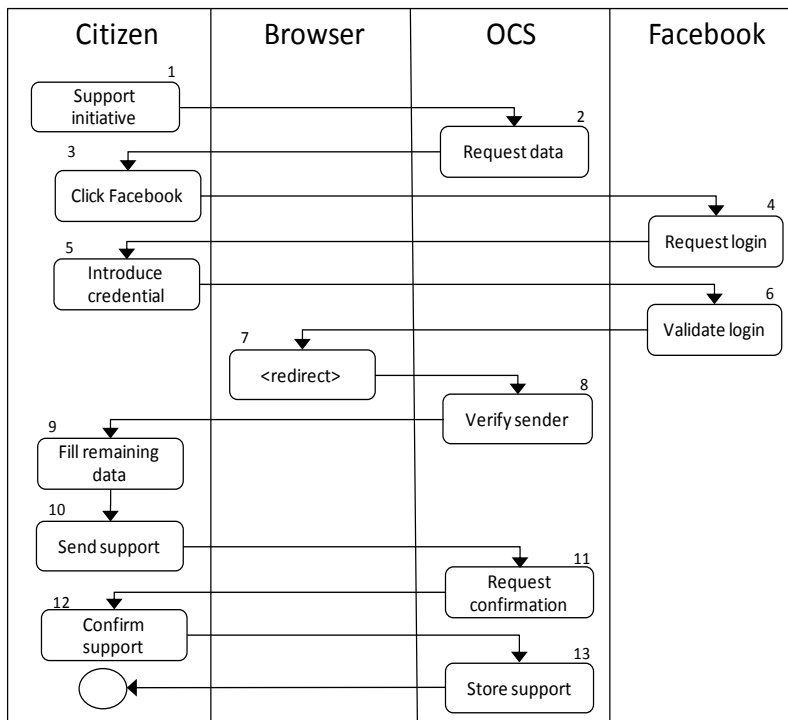


Figure 58: Activity diagram of the collection process

These activities are self-explaining.

18.2 BUSINESS ANALYSIS

Integration of social networks into the OCS mainly has an effect on organisers and citizens. As this complement will not change how the statements of support are collected or verified, the impact on Member State’s verifying authorities is not considered to be significant. The analysis will thus mainly focus on the impact on citizens on each evaluation criterion.

18.2.1 Ease of use

Regarding the user interface, this solution does not present significant differences. However, depending on the data stored, the time devoted to complete the submission, and thus the ease of use of the solution, is different.

Moreover, two-factor authentication methods are becoming popular security features that provide higher degree of certainty on the identity of the user that attempts to gain access to any online service. Facebook provides this method as a way to guarantee only lawful access to its accounts. However, this access is lawful only in the case an authentication procedure is put in place when acquiring phone numbers. In this case, the traditional username and password authentication is combined with a code sent to the user's mobile phone. However, this feature can be enabled by the user and its activation cannot be detected by the receptor of the user's data.

It is also important to consider that this pre-filling options offers the possibility to remove the CAPTCHA, one of the main sources of criticism towards the OCS⁶⁶.

With, more than 1.86 billion users worldwide⁶⁷, Facebook is one of the most widely used social networks. It had 247,070,000 users in the EU in June 2016 (see section 18.2.3 for further information on the penetration level) and is used by a wide variety of citizens from all ages.

The process for retrieving the data is very simple, as the user only has to authorise the retrieval of information from his/her Facebook profile. Once this step is completed, the data fields will be prefilled with the information stored in the Facebook account. The user will have to complete and correct this information in order to comply with the data requirements established by each Member State.

Since the user interface is not impacted by important modifications (only a button to connect with Facebook will be added), and the data will be easily retrieved, this solution will certainly reduce the complexity of the current procedure and the time devoted to finalise it.

18.2.2 Quantity of data (input)

As of today, Facebook users can store the following personal data fields relevant for the ECI requirements: Name, Surname, Date of birth and Address.

Taking into consideration these pieces of data and putting them in contrast with the different personal data currently required by each Member States (as stated in Annex III of the Regulation), the results are diverse, depending on the Member State. Table 52 shows a comparison between both the personal data requirements and the data stored in Facebook accounts.

18.2.3 Penetration level / awareness

When analysing the Facebook complement for the OCS, the facts are more promising. According to Eurostat, 52% of the EU population aged from 16 to 74 was engaged in the use of social networks in 2016.⁶⁸ Specifically, Facebook has penetration rate of 39.5%⁶⁹ in Europe, meaning that over 307

⁶⁶ Anglmayer, Irmgard. (2015) The European Citizen's Initiative: the experience of the first three years. European Parliamentary Research Service.

[http://www.europarl.europa.eu/thinktank/es/document.html?reference=EPRS_IDA\(2015\)536343](http://www.europarl.europa.eu/thinktank/es/document.html?reference=EPRS_IDA(2015)536343). P 10

⁶⁷ <http://www.internetworldstats.com/stats9.htm>

⁶⁸ <http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00127&plugin=1>

million people have a Facebook account⁷⁰. Therefore, implementing a solution that links Facebook, as the main representative of social networks, to the OCS has a significant effect on penetration and will become an excellent tool for the organisers to campaign for an initiative and raise awareness about the ECI tool in general.

⁶⁹ <http://www.internetworldstats.com/facebook.htm>

⁷⁰ <https://zephoria.com/top-15-valuable-facebook-statistics/>

Legend	
x	Present/Required
	Not required/not present
	ECI requirement not present in Facebook

	Name		Fathers' name		Name at birth		Residence		Date of birth		Place of birth		Nationality		Personal Identification Number	
	ECI Personal data requirements	Facebook	ECI Personal data requirements	Facebook	ECI Personal data requirements	Facebook	ECI Personal data requirements	Facebook	ECI Personal data requirements	Facebook	ECI Personal data requirements	Facebook	ECI Personal data requirements	Facebook	ECI Personal data requirements	Facebook
Austria	x	x					with full address details	x	x	x	x		x		x	
Belgium	x	x					x	x	x	x	x		x			
Bulgaria	x	x	x					x		x			x		x	
Croatia	x	x					with full address details	x		x			x		x	
Cyprus	x	x						x		x			x		x	
Czech Republic	x	x						x		x			x		x	
Denmark	x	x					x	x	x	x	x		x			
Estonia	x	x					x	x	x	x	x		x			
Finland	x	x					Only the country	x	x	x			x			
France	x	x					with full address details	x	x	x	x		x		x	
Germany	x	x					x	x	x	x	x		x			
Greece	x	x	x		x			x	x	x			x		x	
Hungary	x	x						x		x			x		x	
Ireland	x	x					x	x	x	x			x			
Italy	x	x					with full address details	x	x	x	x		x		with issuing authority	
Latvia	x	x			x			x	x	x	x		x		x	
Lithuania	x	x						x		x			x		x	
Luxembourg	x	x					with full address details	x	x	x	x		x			
Malta	x	x						x	x	x			x		x	
Netherlands	x	x			x		x	x	x	x	x		x			
Poland	x	x					with full address details	x		x			x		x	
Portugal	x	x						x	x	x			x		x	
Romania	x	x					with full address details	x	x	x			x		x	
Slovakia	x	x			x		x	x	x	x	x		x			
Slovenia	x	x						x	x	x	x		x		x	
Spain	x	x						x	x	x			x		x	
Sweden	x	x						x		x			x		x	
UK	x	x					x	x	x	x			x			

Table S2: Comparison between the ECI personal data requirements and the data stored in Facebook accounts

This comparison table shows that, for some countries, the amount of data to be added is minimal whereas for others that quantity is higher.

For instance, citizens from Finland will only need to type in their nationality, as the rest of the data required by those countries could be retrieved from the signatory's Facebook account. However, citizens from countries that require additional data such as Identification number (Austria, France, Spain, Sweden, etc.), place or birth (e.g. Belgium, Denmark, Estonia or Slovakia), name at birth (Latvia, the Netherlands and Slovenia) or father's name (Bulgaria and Greece) have to provide additional of data in order to complete the submission.

When analysing the data that will be covered by the information stored in Facebook profiles, it is important to note that all the data stored in Facebook is optional. As a result, the data to be inserted will ultimately depend on what amount of data each citizen has stored in his/her Facebook account. In cases the information is not accurate, the user has to correct the fields that do not display accurate data, increasing the final amount of data to be inserted.

18.3 TECHNICAL ANALYSIS

18.3.1 Ease of integration

The changes to apply to the OCS relate to two areas:

- The navigation: These are minor changes, which will not present any problems to integrate.
- The inclusion of the Facebook Login module: The integration of the Facebook Login module requires a call to its API, enumerating the requested attributes. The result is a call from this system, returning attribute name / value pairs. Complete documentation of the OAuth 2.0 protocol is available on the Internet. It has been integrated and has been tested in many websites; important integration problems are not expected.

18.3.2 Scalability

As mentioned, the OCS is extended with the Facebook Login module, in charge of the following functions:

- Composing and sending the authentication request to the Facebook login system
- Receiving the response and extracting the data from this response.

These functions do not present any scalability issues: new types of eIDs can be included without affecting the integration in the OCS.

18.3.3 Maintainability

The Facebook Login module, once integrated into the OCS, is not expected to suffer changes over time, neither for the specifications of its API, nor for the supported data. No maintenance on these integrations is therefore expected.

18.3.4 Performance and usage of resources

These solutions impact on the required resources regarding the CPU usage. If 20% of the statements of support would use the feature of Facebook Login, the validation of the signature included in the response from the Facebook Login system would cause an increase of the CPU consumption of around 14%, based on performance tests in the STORK project. Based on the same tests, the total amount of authentication transactions is estimated in around 50 per second, which is equivalent to over 4 million per day.

18.3.5 Security

This integration is designed to facilitate the filling of the support form of the OCS. As such, no changes in the security performances are anticipated. The only noticeable improvement is the possibility to remove the captcha feature for the users who would choose to integrate with EU Login.

Compared with the current situation, this solution offers no additional guarantees against citizens voting more than once, on behalf of other people, nor against EU residents from non-EU countries supporting initiatives.

18.3.6 Maturity

Integration with Facebook has been performed for several years by many organisations, so this solution is considered mature.

18.3.7 Portability

This tool is accessible on multiple platforms as they are implemented as web applications. No issues are expected.

18.3.8 Costs / efforts

The little complexity of the Facebook Login module and its API motivate the efforts required for the inclusion of these modules into the OCS to be estimated as low. Additionally, the large experience of integration of this solution into applications of many organisations motivates even more the confidence in a smooth integration.

The efforts required to include Facebook Login into the OCS involve changes in the navigation and inclusion of the Facebook Login modules. They are estimated around 3 man-months.

19 APPENDIX H – EVALUATION MATRIX

19.1 EVALUATION MATRIX – SOLUTION 1

Dimension	Evaluation criteria	Domain/Stakeholder	Ideal Example	Description/Justification	Score	
Legal analysis	ECI Regulation	Submission of statement of support	The submission of statement of support can be carried out as proposed in the solution within the current legislative framework (Article 5 and 6).	The Regulation foresees the use of electronic signatures, and the OCS will comply with the requirements of Art.6.4. Only a change in Annex III could be promoted.	5.00	
		Verification of statement of support	The solution proposes a verification method that is compliant with Article 8.	Article 8 mentions electronic signatures when establishing the differentiation of the alternatives available for signing a statement of support.	5.00	
		Data protection	When this solution is implemented, the OCS still complies with the requirements for data protection stated in Article 12.	The way the data stored will not be changed under this solution. The modifications needed in the OCS will still comply with the requirements of Article 12, as the data stored will be just included in the certificate, making it less prone to be used unlawfully.	5.00	
	Average Score					5.00
	eIDAS Regulation	NA	Where applicable, the solution complies with the eID/eSignature standards.	The use of eSignature for the purpose of ECI is compliant with the Regulation. Advanced electronic signatures are already mentioned in the Regulation. Also, if a modification in Annex III is made, qualified electronic signatures could also be used.	5.00	
	Average Score					5.00
	Member States	Question 1	Member States are willing to reduce their data requirements in order to simplify the process to submit a statement of support.	Approximately 30% of the consulted sources are willing consider some of the data as optional, another 30% percent consider that they could not reduce the requirements of Annex III, while the rest of them could not provide an answer in the moment.	3.00	
		Question 2	The penetration level of electronic signature is high, proving the suitability of the solution for implementation.	50% of the countries have responded that electronic signature is issued to the majority of their population (for some even the total population over 18years old). Some of the countries who responded no showed that electronic signature is becoming more popular, what shows a growing trend across MS.	4.00	
		Average Score				
	Business Analysis	Ease of Use	Citizens (user interface)	The solution does not require any extra software or hardware component to function, and its supported by different internet browsers and operative systems. When the user makes use of this solution, the process can be completed in a quick way through a smooth user interface, reducing the number of clicks needed to support an initiative.	The user interface will be slightly modified, but the process itself could be more time consuming if the user has to go through the alternative flows presented (pre-filling options).	2.00
Organisers			The solution does not change the OCS in a way it is more difficult to collect and store statements of support.	Organisers will be provided with a more secure alternative for collecting statements of support. In addition, this solution provides them with the possibility to use electronic signature when sending the statements of support for verification.	4.00	
Verification authorities			The solution fosters the creation of statements of support with a high degree of confidence in the validity of the data corresponding to the signatory, easing the task of verification by MS authorities and the issuing of the certificate presented in Annex VI of the ECI Regulation.	V.A. will receive statements of support based on certificates that are uniquely linked to the signatory, whose identity can be verified easily by checking the validity of the certificates. The statements of support will not be automatically validated.	3.00	
Average Score					3.00	
Quantity of Data (input)		Citizens (user interface)	The solution reduces the amount of data to be typed in. The data used can be securely transmitted and stored. There is good reliability.	Solution 1 will allow citizens to submit a statement of support by using only a e-signature certificate. The pre-filling options will also decrease the amount of data to be input in case the user has to go through the alternative flow.	3.00	
		Organisers	The solution has a positive effect on the way they manage the data collected within the statements of support.	Organisers will be provided with a more secure alternative for collecting statements of support. In addition, this solution provides them with the possibility to use e-signature when sending the statements of support for verification.	4.00	
		Verification authorities	The solution eases the task of verification of the identity of signatories by MS verification authorities, as statements of support will be automatically validated or the process to check the data against national databases is simplified.	Verification authorities will still need to verify the identity of signatories checking the validity of certificates, Although the data will be retrieved from trustworthy sources (advanced/qualified e-signature certificates)	4.00	
Average Score					3.67	
Penetration Level/Awareness		Citizens (user interface)	The e-signature solution is available to a major percentage of the population and has several applications besides submitting a statement of support.	This criteria consider the availability of both electronic signatures and PDF tools. Although all countries issue qualified certificates, only 50% of the MS consulted can assure that electronic signature is issued to the majority of adult population. Some MS have indicated a growing trend regarding its use. On the other hand, PDF handling tools are very common and well spread.	3.00	
		Organisers	Organisers will not suffer a negative impact on their activities when the solution is implemented.	The reduced legal risks, the enhanced security and user-friendly interface will be beneficial for organisers, although this effect will be indirect.	3.00	
	Verification authorities	Implementing a solution that is penetrated affects the validation in a way that, by receiving statements of support containing data that comes from popular and trustworthy sources, the verification of such data is smooth and accessible.	The electronic signature tool selected will be the one with the highest penetration level in each MS. Therefore, verification authorities will receive data from an encrypted trustworthy source that can clearly establish the identity of a signatory. Nonetheless, current penetration rate amongst citizens limits the overall scoring for the verification authorities	3.00		
Average Score					3.00	

Technical Analysis	Scalability	Considering that citizens are completely identified by their qualified signature, in principle the MS specific modules could be omitted. Thus no scalability issues are found with this solution.	Considering that citizens are completely identified by their qualified signature, in principle the MS specific modules could be omitted. New eIDs are accepted without any effort. New eIDs are accepted without any effort; new MS would require little integration effort.	5.00
	Maintainability	No maintainability issues can be expected.	No changes can be foreseen in the TSLs and PDF/PAdES specifications.	5.00
	Performance & usage of resources	The CPU usage will increase in an important percentage, but the throughput of a modern server is more than enough to support several initiatives in parallel	The CPU usage will increase in an important percentage (around 70%) because of the resources needed for the certificate and signature verification, but the CPU throughput of a modern server is more than enough to support many initiatives in parallel. Performance tests in the STORK project have shown that a modern server can produce and verify some 50 signatures per second, which is 80.000 signatures per day.	4.00
	Average Score- Operational aspects			4.67
	Security on data storage	If the current security measures are extended to the new attributes, no important issues can be expected	The current security measures comply with the requirements from the Regulation and the EC security policy.	4.00
	Fraud prevention	Fraud prevention is improved as the signature binds the statement of support to one specific initiative.	As a statement of support is linked to a specific initiative, copying statements of support from one initiative to another is detected. The signature binds the statement of support to one specific initiative.	4.00
	Security on data transmissions	The integrity of the data transmissions is improved.	The integrity of the data transmissions is improved, because changes in the data during the transmission can be detected as the signature would become invalid.	4.00
	Session management	Session management is improved, as the statement of support is transmitted in one http session, without the need for corrections.	The statement of support is transmitted in one http session. The management of the relation between this session and the conformation of the support uses standard mechanisms.	4.00
	Average Score- Security			4.00
	Ease of integration	Considering that citizens are completely identified by their qualified signature, in principle the MS specific modules could be omitted. In that case one simple module for checking the certificate should be used. Additionally, the integration of PDF manipulation libraries is expected not to produce any problem.	Experiences in EC financed project like STORK have shown that the PDF manipulation libraries are easy to integrate. The creation of signatures is located outside the OCS, so needs no integration effort.	4
	Maturity	The solution is mature; all underlying technologies exist on the market since several years.	- PDF is the most commonly used standard for document exchange on the Internet - PAdES is the commonly accepted standard for signatures on PDF documents - most PDF readers support producing advanced signatures on documents	5.00
	Portability	The solution with Java is portable with little effort.	Considering that this solution will be implemented in Java (back-end), and in HTML and Angular (front-end), it is portable with little effort.	4.00
	Cost/Efforts	The implementation of the solution only requires minor changes in the ECI online collection systems and no change at all at MS level.	This solution can be implemented with a moderate cost. Estimations are around 4-5 man-months	4.00
	Average Score- Integration			4.33

19.2 EVALUATION MATRIX – SOLUTION 2

Dimension	Evaluation criteria	Domain/Stakeholder	Ideal Example	Description/Justification	Score	
Legal analysis	ECI Regulation	Submission of statement of support	The submission of statement of support can be carried out as proposed in the solution within the current legislative framework (Article 5 and 6).	This solution is feasible within the ECI regulation as far as the e-signature certificates used are compliant with the eIDAS Regulation. However, a modification of Annex III is required to include a separate form that foresees the use of e-signature.	4.00	
		Verification of statement of support	The solution proposes a verification method that is compliant with Article 8.	Although the use of e-signature is mentioned in the verification process, it is recommendable to amend Article 8 with a specific mention of the automatic validation of the data retrieved from e-signatures. Besides, Annex III should also be modified, adding a specific criteria for the statements of support submitted via e-signature.	4.00	
		Data protection	When this solution is implemented, the OCS still complies with the requirements for data protection stated in Article 12.	The data retrieved is specifically linked to the signed statement of support and cannot be used for any other purposes. Moreover, no change in the way the data is managed, stored and later, destroyed is foreseen for this solution. Therefore, this solution complies with Article 12 of the Regulation.	5.00	
	Average Score					4.33
	eIDAS Regulation	NA	Where applicable, the solution complies with the eID/eSignature standards.	Qualified certificates offer the highest level of assurance as it is controlled and managed by the Member States, therefore being compliant with the Regulation, improving reliability of the data.	5.00	
	Member States	Question 1	Every statement of support submitted using e-signature is flagged and then sent to the national verification authorities with this flag, indicating the automatic validation of the data contained in the statement of support.	The Member States are clearly in favour of the establishment of the flag to indicate the validation of the data from the signatory. From a legal point of view, establishing this flag can be carried out when implementing an integration of the eSignatures CEF Building Block into the Online Collection System	5.00	
		Question 2	The process of submitting the statements of support to the verification authorities remains the same, compliant with the verification and validation procedure detailed in the Regulation.	Verification authorities would be willing to continue with the current procedure and receive the statements of support to possibly perform additional checks. Some concerns regarding the manipulation of the flag by the organisers have been raised by some Member States, but could easily be overcome by including electronic timestamp.	5.00	
		Question 3	Some of the personal data requirements of Annex III are considered optional, making sure the data contained in the e-signature is sufficient. No additional data is required from the user.	A third of the consulted Member States is in favour of reducing the amount of data required in Annex III. However, another third shows resistance to this possibility.	3.00	
		Question 4	e-signature is issued to the majority of the European population, proving the suitability of the solution for implementation.	In half of the consulted Member States, e-signature certificates are issued to the majority of the national population while in a quarter of the countries it is not the case. However, those Member States indicated a growing trend and an increasing demand across Europe.	4.00	
	Average Score					4.40
Business Analysis	Ease of Use	Citizens (user interface)	The solution does not require any extra software or hardware component to function, and it is supported by different internet browsers and operative systems. When the user makes use of this solution, the process can be completed in a quick way through a smooth user interface, reducing the number of clicks needed to support an initiative.	This solution does not necessarily require any piece of hardware and specific software to work, provided that users have a certificate stored in their internet browsers. The process will be smooth, fast and user friendly	5.00	
		Organisers	The solution does not change the OCS in a way it is more difficult to collect and store statements of support.	Solution 4 does not significantly change the way SoS are stored or managed.	3.00	
		Verification authorities	The solution fosters the creation of statements of support with a high degree of confidence in the validity of the data corresponding to the signatory, easing the task of verification by MS authorities and the issuing of the certificate presented in Annex VI of the ECI Regulation.	Qualified certificates provide a high level of assurance on the identity of signatories. Therefore, data will be retrieved from trusted sources and the validation task will be facilitated	5.00	
	Average Score					4.33
	Quantity of Data (input)	Citizens (user interface)	The solution reduces the amount of data to be typed in. The data used can be securely transmitted and stored. There is good reliability.	By using qualified certificates, the quantity of data is reduced to zero	5.00	
		Organisers	The solution has a positive effect on the way they manage the data collected within the statements of support.	Data from e-signatures is encrypted and more difficult to be used for unlawful purposes, providing additional security for organisers when they manage large quantities of statements of support	4.00	
		Verification authorities	The solution eases the task of verification of the identity of signatories by MS verification authorities, as statements of support will be automatically validated or the process to check the data against national databases is simplified.	e-signature-based statements of support will be validated when retrieving the data from national databases. Therefore at the end of the collection phase the number of statements of support to be validated is reduced	4.00	
	Average Score					4.33
	Penetration Level/Awareness	Citizens (user interface)	The e-signature solution is available to a major percentage of the population and has several applications besides submitting a statement of support.	Although all countries issue qualified certificates, only 50% of the MS consulted can assure that e-signature is issued to the majority of adult population. Some MS have indicated a growing trend regarding its use.	2.00	
		Organisers	Organisers will not suffer a negative impact on their activities when the solution is implemented.	The fact that e-signature is implemented can have indirect positive effects, (overall awareness of ECI, willingness of citizens to submit statements of support, etc.). These effects are difficult to assess individually.	3.00	
Verification authorities		Implementing a solution that is penetrated affects the validation in a way that, by receiving statements of support containing data that comes from popular and trustworthy sources, the verification of such data is smooth and accessible.	Qualified certificates provide the most secure and reliable data (controlled by Member States through trust lists). In addition, the Commission released the first eIDAS-compliant version of its DSS early May, making it possible to verify any electronic signature from users of any Member State seamlessly. However, only few Member States have released an updated eIDAS-compliant version of their electronic signature.	3.00		
Average Score					2.67	

Technical Analysis	Scalability		The e-signature service can accommodate a growing number of requests with any change to the architecture.	The e-signature service provided by the Commission (DSS) is scalable as it performs the validation of the signature itself and does not rely on Member State's specific modules to validate the certificate or extract the user's data.	5.00
	Maintainability		Maintainability issues can be expected in the Member States' specific modules.	Any change in the specifications of any of the eIDs or their validation method would require a change in its corresponding module.	4.00
	Performance & usage of resources		The CPU usage will increase in an important percentage, but the throughput of a modern server is more than enough to support several initiatives in parallel	The CPU usage will increase in an important percentage, but the throughput of a modern server is more than enough to support several initiatives in parallel. Performance tests in the STORK project have shown that a modern server can produce and verify some 50 signatures per second, which is 80.000 signatures per day.	4.00
	Average Score-Operational Aspects				4.33
	Security on data storage		The security of data storage is improved, as the signature guarantees the integrity of the Statements of Support	The current security measures comply with the requirements from the Regulation and the EC security policy.	4.00
	Fraud prevention		Fraud prevention is improved, as citizens can't support on behalf of other persons.	Fraud prevention is improved, as citizens can't support on behalf of other persons. Statements of support cannot be copied from one initiative to others. However, most eIDs don't include the nationality of the citizen, so citizens from outside the EU could vote.	4.00
	Security on data transmissions		The integrity of the data transmissions is improved, as the signature guarantees the integrity of each statement of support	This solution provides a secure transmission mechanism.	4.00
	Session management		Session management is improved, as the statement of support is transmitted in one http session, without the need for corrections.	The statement of support is transmitted in one http session. The management of the relation between this session and the conformation of the support uses standard mechanisms.	4.00
	Average Score-Security				4.00
	Ease of integration		This solution is complex to integrate. If the Member States' specific modules would not perform the validation of the certificate, nor the extraction of the user's data, this solution would be moderate to integrate. The signature creation tool is complex to configure and integrate.	The Member States' specific modules are complex due to the validation and extraction functions, and there are 28 such modules.	3.00
	Maturity		The solution is mature; all underlying technologies exist on the market since several years.	e-signature has been present in the EU for some years and the penetration level is optimal for implementation. On the other hand, the DSS solution has been recently developed, and might still face some operational issues.	3.00
	Portability		The solution with Java is portable with little effort.	The solution with Java is portable with little effort. Java can be ported to other operating systems, mostly even without recompiling. Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different application servers.	5.00
	Cost/Efforts		The implementation of the solution only requires minor changes in the ECI online collection systems and no change at all at MS level.	The cost/effort estimations are around 12 man-months.	3.00
	Average Score- Integration				3.67

19.3 EVALUATION MATRIX – SOLUTION 3

Dimension	Evaluation criteria	Domain/Stakeholder	Ideal Example	Description/Justification	Score	
Legal analysis	ECI Regulation	Submission of statement of support	The submission of statement of support can be carried out as proposed in the solution within the current legislative framework (Article 5 and 6). The solution proposes a verification method that is compliant with Article 8.	This solution considers a possibility of change of the Regulation, requiring a mention of the use of eID to support a statement of support in order to be compliant with Article 6.4.	3.00	
		Verification of statement of support		The statements of support are sent online to the verification authorities, in accordance with Article 8.1, following the form set out in Annex V. However, an amendment of Article 8 would be advisable to include a mention about automatic validation of the data retrieved from eIDs. In addition, a specific criteria regarding statements of support submitted via eID should be added in Annex III.	2.00	
		Data protection	When this solution is implemented, the OCS still complies with the requirements for data protection stated in Article 12.	No change is anticipated in the way the personal data of signatories is managed in this solution. Therefore, both the organisers and the verification authorities comply with the Regulation regarding data protection and no additional information than the one strictly necessary for the support of an initiative is retrieved from the eID.	5.00	
	Average Score					3.33
	eIDAS Regulation	NA	Where applicable, the solution complies with the eID/eSignature standards.	Not applicable for this solution. The in-depth eIDAS analysis is carried out in solution 3	NA	
	Member States	Question 1	The flag would indicate that data has already been validated in order to prevent checking twice the same information .	Member States are in favour of this option, which is legally compliant when implementing direct integration of eID.	5.00	
		Question 2	The process of sending the statements of support to the verification authorities of each MS is still applicable. Even though the "flag system" is used, the verification and validation process is still followed, to be compliant with the Regulation.	Despite the use of the flag, verification authorities are still willing to receive the statements of support in order to have the possibility to perform an additional check to account, for example, for duplicates. The same verification and validation process is thus still applied.	5.00	
		Question 3	Some of the personal data requirements of Annex III are considered optional, making sure the data contained in the eID is sufficient to support an initiative. No additional data is required from the user.	More than a third of the responses from the Member States shows that they are willing to promote the use of eID to support an ECI and therefore inclined to adjust their personal data requirements. However, another third indicates resistance to this possibility.	2.00	
		Question 4	eID is only issued to natural persons and not to legal persons. Consequently, only EU citizens have the possibility to support an ECI.	Only one of the consulted Member States is issuing eIDs certificates to legal persons. However, the competent authorities have the possibility to differentiate legal and natural persons, therefore preventing any unlawful use of the ECI.	5.00	
		Question 5	Interactive verification is present in the most majority of the EU Member States.	Only one out of the twelve respondents mentioned that this interactive verification is not possible in their Member State. In the others, automatic validation is already implemented.	4.00	
Average Score					4.20	
Business Analysis	Ease of Use	Citizens (user interface)	The solution does not require any extra software or hardware component to function, and its supported by different internet browsers and operative systems. When the user makes use of this solution, the process can be completed in a quick way through a smooth user interface, reducing the number of clicks needed to support an initiative.	Connecting with eID will require a specific piece of hardware (card reader) in those Member States whose most popular eID tool is a smart card. Nevertheless, the process will be smooth, user friendly and fast, requiring little time to be completed .	4.00	
		Organisers	The solution does not change the OCS in a way it is more difficult to collect and store statements of support.	Statements of support will be stored together with the flag that accounts for automatic validation. No difference is expected in the way organisers manage collection and delivery of statements of support.	5.00	
		Verification authorities	The solution fosters the creation of statements of support with a high degree of confidence in the validity of the data corresponding to the signatory, easing the task of verification by MS authorities and the issuing of the certificate presented in Annex VI of the ECI Regulation.	Given the fact that statement of support will be validated when connecting to the national eID database, this will reduce the number of statements of support that would require verification once the collection phase has ended.	4.00	
	Average Score					4.33
	Quantity of Data (input)	Citizens (user interface)	The solution reduces the amount of data to be typed in. The data used can be securely transmitted and stored. There is good reliability.	Users will only need to connect to the correspondent eID database and allow for the retrieval of data. The quantity of data to be input is reduced to zero.	5.00	
		Organisers	The solution has a positive effect on the way they manage the data collected within the statements of support.	Data retrieved from national eID databases will be flagged. Assuming verification authorities will consider those as automatically validated, it will give organisers a more clear idea on the actual number of valid statements of support collected.	3.00	
		Verification authorities	The solution eases the task of verification of the identity of signatories by MS verification authorities, as statements of support will be automatically validated or the process to check the data against national databases is simplified.	Statements of support based on data retrieved from eID will be flagged, and could be considered as 'de facto' validated. Even though verification authorities will still receive them, this solution will have a major impact in their task, as it would create an important reduction in the statements of support that need to be validated.	4.00	
	Average Score					4.00
	Penetration Level/Awareness	Citizens (user interface)	The eID solution is available to a major percentage of the population and has several applications besides submitting a statement of support.	Almost all MS have implemented or will implement an eID scheme. More than 50%of the consulted MS assured that eID was issued to the majority of their adult population. Some of the rest have reported a growing number of citizens using eIDs.	4.00	
		Organisers	Organisers will not suffer a negative impact on their activities when the solution is implemented.	Effect for organisers (enhanced overall performance, reduced legal risks) might be indirect and difficult to assess individually.	3.00	
Verification authorities		Implementing a solution that is penetrated affects the validation in a way that, by receiving statements of support containing data that comes from popular and trustworthy sources, the verification of such data is smooth and accessible.	Organisers will receive statements of support coming from the eID solution with the highest penetration level in their own country. Therefore, verification task will be eased and their task will be eased.	4.00		
Average Score					3.67	

Technical Analysis	Scalability	Scalability issues exist in the Member States' specific modules. If the Member States' specific modules would not perform the validation of the certificate, nor the extraction of the user's data, this solution would be perfectly scalable.	Scalability issues exist in the Member State's specific modules. New eIDs would require new Member States' specific modules; new Member States would also require new modules.	1.00
	Maintainability	Maintainability issues can be expected in the Member States' specific modules.	Any change in the specifications of any of the eIDs or their validation method would require a change in its corresponding module.	1.00
	Performance & usage of resources	The CPU usage will increase in an important percentage, but the throughput of a modern server is more than enough to support several initiatives in parallel	A modern server can produce and verify around 50 signatures per second, which is 80.000 signatures per day. If the CPU usage would be a bottle-neck, several servers could be used in parallel.	4.00
	Average Score- Operational Aspects			2.00
	Security on data storage	If the current security measures are extended to the new attributes, no important issues can be expected	The current security measures comply with the requirements from the Regulation and the EC security policy.	4.00
	Fraud prevention	Fraud prevention is improved, as citizens can't support on behalf of other persons.	Fraud prevention is improved, as citizens cannot register support on behalf of other persons. However, most eIDs don't include the nationality of the citizen, so additional rules must be implemented to prevent citizens from non-EU countries to vote in case they have an eID card/token from their EU country of residence.	3.00
	Security on data transmissions	The integrity of the data transmissions remains unaltered.	This solution provides a secure transmission mechanism.	4.00
	Session management	Session management is improved, as the statement of support is transmitted in one http session, without the need for corrections.	The statement of support is transmitted in one http session. The management of the relation between this session and the conformation of the support uses standard mechanisms.	4.00
	Average Score-Security			3.75
	Ease of integration	This solution is integrated seamlessly into the OCS workflow.	The Member States' specific modules are complex due to the validation and extraction functions, and there should be at least 28 such modules. Furthermore, in countries with several eID providers (i.e. Spain), a broader coverage will be achieved only with the implementation of a connector for each provider, which means also extra evolutive maintenance whenever a new eID provider is registered.	1.00
	Maturity	The solution is mature; all underlying technologies exist on the market since several years.	eIDs are available, or will soon be implemented, in all Member States.	4.00
	Portability	The solution with Java is portable with little effort.	Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different application servers. However, this has to be repeated for each connectors.	3.00
	Cost/Efforts	The implementation of the solution only requires minor changes in the ECI online collection systems and no change at all at MS level.	Implementation costs are high. Estimations are between 20 to 25 man-months.	1.00
	Average Score- Integration			2.25

19.4 EVALUATION MATRIX – SOLUTION 4

Dimension	Evaluation criteria	Domain/Stakeholder	Ideal Example	Description/Justification	Score	
Legal analysis	ECI Regulation	Submission of statement of support	The submission of statement of support can be carried out as proposed in the solution within the current legislative framework (Article 5 and 6).	As this solution considers a possibility of change of the Regulation, a specific mention of eID to submit a statement of support, as well as to the eIDAS Regulation, should be added to provide proper legal basis for its implementation. Moreover, the model for creating a statement of support is updated to include only the data shared within the eIDAS framework (Art. 6). A modification of Annex III is also recommended to include the possibility to use eID to submit a statement of support.	2.00	
		Verification of statement of support	The solution proposes a verification method that is compliant with Article 8.	The form set out in Annex V is still applicable in this solution. Article 8 would however require a modification to include a reference to the automatic validation of the data through eIDAS. Annex III should also be modified to add a specific criteria for the statements of support submitted via eID.	3.00	
		Data protection	When this solution is implemented, the OCS still complies with the requirements for data protection stated in Article 12.	No change in the way data is managed and destroyed is foreseen for this solution and the OCS will include all the necessary security measures to ensure the protection of the data. This solution can therefore be implemented without any change in the Regulation regarding data protection.	5.00	
	Average Score					3.33
	eIDAS Regulation	NA	Where applicable, the solution complies with the eID/eSignature standards.	The use of authentication methods (eID) for the purpose of supporting eID falls within the scope of eIDAS within the implementation of this solution. Main components of this solution are fully compliant with the eIDAS Regulation, as data protection is guaranteed and the level of assurance of the selected eID solutions is ranked as substantial or high in the majority of Member States	5.00	
	Member States	Question 1	Nationality, as a key element to support an ECI, is part of the data shared through eIDAS by Member States.	There is no general agreement among the Member States regarding the sharing of nationality but half of the consulted countries were positive about sharing this information. For some countries, nationality can easily be extracted from the Unique Identifier Number while some cannot provide a definitive answer at the moment.	4.00	
		Question 2	The eIDAS Unique Identifier is sufficient to establish the identity of the signatories.	Member States are generally against the possibility of only using the Unique Identifier to establish the identity of the user. On the other hand, many have shown the possibility of using only the Minimum Set of Data to identify a person	2.00	
		Question 3	Member States are willing to share the place of birth and the residence address in the eIDAS network.	Half of the consulted Member States confirmed they would agree on sharing those information.	4.00	
	Average Score					3.33
	Business Analysis	Ease of Use	Citizens (user interface)	The solution does not require any extra software or hardware component to function, and its supported by different internet browser and operative systems. When the user makes use of this solution, the process can be completed in a quick way through a smooth user interface, reducing the number of clicks needed to support an initiative.	connecting with eID will require a specific piece of hardware (card reader) in those Member States whose most popular eID tool is a smart card. Nevertheless, the process will be smooth, user friendly and fast, requiring little time to be completed.	4.00
Organisers			The solution does not change the OCS in a way it is more difficult to collect and store statements of support.	Statements of support will be stored together with the flag that accounts for automatic validation. No difference is expected in the way organisers manage collection and delivery of statements of support.	5.00	
Verification authorities			The solution fosters the creation of statements of support with a high degree of confidence in the validity of the data corresponding to the signatory, easing the task of verification by MS authorities and the issuing of the certificate presented in Annex VI of the ECI Regulation.	Given the fact that statement of support will be validated when connecting to the national eID database, this will reduce the number of statements of support that would require verification once the collection phase has ended.	4.00	
Average Score					4.33	
Quantity of Data (input)		Citizens (user interface)	The solution reduces the amount of data to be typed in. The data used can be securely transmitted and stored. There is good reliability.	users will only need to connect to the correspondent eID database and allow for the retrieval of data. The quantity of data to be input is reduced to zero.	5.00	
		Organisers	The solution has a positive effect on the way they manage the data collected within the statements of support.	Data retrieved from national eID databases will be flagged. Assuming verification authorities will consider those as automatically validated, it will give organisers a more clear idea on the actual number of valid statements of support collected.	3.00	
		Verification authorities	The solution eases the task of verification of the identity of signatories by MS verification authorities, as statements of support will be automatically validated or the process to check the data against national databases is simplified.	flagged statements of support, could be considered as 'de facto' validated. Even though verification authorities will still receive them, this solution will have a major impact in their task, as it would create an important reduction in the statements of support that need to be validated.	4.00	
Average Score					4.00	
Penetration Level/Awareness		Citizens (user interface)	The eID solution is available to a major percentage of the population and has several applications besides submitting a statement of support.	Although eID is widely penetrated in the EU, only three countries so far have successfully achieved interconnection of their eIDAS nodes. Some countries are immersed in the testing phase. By 2018, all MS nodes should be fully operational.	4.00	
		Organisers	Organisers will not suffer a negative impact on their activities when the solution is implemented.	Effect for organisers (enhanced overall performance, reduced legal risks) might be indirect and difficult to assess individually.	3.00	
		Verification authorities	Implementing a solution that is penetrated affects the validation in a way that, by receiving statements of support containing data that comes from popular and trustworthy sources, the verification of such data is smooth and accessible.	Organisers will receive statements of support coming from the eID solution with the highest penetration level in their own country. Therefore, verification tasks will be easier to carry out.	4.00	
Average Score					3.67	

Technical Analysis	Scalability	No scalability issues exist.	New eIDs or new Member States would not require any change in the OCS	5.00
	Maintainability	No maintainability issues are expected.	Any change in the specifications of any of the eIDs or their validation method would not require any change in the OCS.	5.00
	Performance & usage of resources	The CPU usage will increase in an important percentage, but the throughput of a modern server is more than enough to support several initiatives in parallel	Performance tests in the STORK project have shown that a modern server can produce and verify some 50 signatures per second, which is 4M signatures per day.	4.00
	Average Score- Operational Aspects			4.67
	Security on data storage	If the current security measures are extended to the new attributes, no important issues can be expected	The current security measures comply with the requirements from the Regulation and the EC security policy.	4.00
	Fraud prevention	Fraud prevention is improved, as citizens can't support on behalf of other persons.	Fraud prevention is improved, as citizens can't support on behalf of other persons. However, eIDAS does not include the nationality of the citizen, so citizens from outside the EU could vote. Statements of support could be	3.00
	Security on data transmissions	The transmission of data from the eIDAS network to the OCS is improved. The transmission of data from the organisers to the verification authorities remains the same.	The eIDAS network guarantees confidentiality with encryption, and the integrity with signatures.	4.00
	Session management	Session management is improved, as the statement of support is transmitted in one http session, without the need for corrections. Additionally, the SAML response is checked to be a reply to the request.	The statement of support is transmitted in one http session. The management of the relation between this session and the conformation of the support uses standard mechanisms. The attribute of the SAML response "InReplyTo" must have the same value as the Id of the request.	5.00
	Average Score- Security			4.00
	Ease of integration	This solution is easy to integrate.	Only one module with a simple API is to be integrated. Examples for integration are available.	5.00
	Maturity	The solution is not mature: some nodes are available in production, but no eID has been notified.	Only one eID has been pre-notified (Germany), and several others will be prenotified this year.	2.00
	Portability	The solution with Java is portable with little effort.	Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different application servers.	5.00
	Cost/Efforts	The implementation of the solution only requires minor changes in the ECI online collection systems and no change at all at MS level.	This solution can be implemented with a low cost. Estimations are around 3 man-months	5.00
	Average Score- Integration			4.00

19.5 EVALUATION MATRIX – SOLUTION 5

Dimension	Evaluation criteria	Domain/Stakeholder	Ideal Example	Description/Justification	Score	
Data Privacy	Data Privacy	NA	The personal information of the user are safely stored, passwords are encrypted and the security features make the solution suitable for a potential integration with the OCS.	Only personal information entered manually by the user or provided by the public organisation him/her belongs to when granting access to the system is stored. the EC will not divulge the information with two exceptions: <ul style="list-style-type: none"> The duly authorised support unit or help desk. Duly authorised bodies, on a case by case basis (eg. Internal Commission Security Directorate) Passwords are encrypted and stored only in a reversible form. EU Login presents security features that make it a suitable solution for a potential integration with the OCS.	5.00	
	Ease of Use	NA	The solutions is able to prefill data in a smooth and user friendly way, reducing the time devoted to submit a statement of support.	The user will have to give his/her consent for the retrieval of data. In a few clicks, and after entering his username/password (and possibly go through the two-step authentication) the data will be pre-filled in the OCS. If the two step authentication is used, the user would not be required to complete the captcha before submitting the statement of support	2.00	
Business Analysis	Quantity of Data (input)	NA	The pre-filling solution is able to include a substantial quantity of the data requirements, reducing the fields that the user needs to type in manually	EU Login external accounts currently store very little information about citizens. Therefore, the user will still need to enter most to the data fields manually	1.00	
	Penetration Level/Awareness	NA	The pre-filling solution is based on an account very penetrated at EU level, meaning that a significant amount of citizens across MS will be able to make use of this solution	EU Login is a fairly new service that is not currently used by a significant part of the EU population	1.00	
	Scalability	NA	The solution is able to handle a growing number of MS and signatories without requiring any changes to the architecture of the solution.	No scalability issues exist. New eIDs or new Member States are irrelevant for this solution	5.00	
Technical Analysis	Maintainability	NA	Any component of the solution can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment without requiring a redesign or refactoring of the system architecture.	No maintainability issues are expected. The specifications of both solutions are not expected to change	5.00	
	Performance & usage of resources	NA	The solution does not impact the performance of the system for the end users and it is able to handle a higher load with an increase of the infrastructure proportional to the total number of users	The CPU usage will increase in an important percentage (around 70%), but the throughput of a modern server is more than enough to support many initiatives in parallel. Performance tests in the STORK project have shown that a modern server can produce and verify some 50 signatures per second, which is 4M signatures per day.	4.00	
	Average Score-Operational Aspects					4.67
Technical Analysis	Security on data storage	NA	All data collected through the ECI online collection system is securely stored so that: - it cannot be accessed by unauthorised users; - it cannot be tampered by anybody (EU citizens, ECI organisers, system administrators, etc.), and; - it won't be lost or destroyed.	No change	3.00	
	Fraud prevention	NA	The solution prevents potential fraud scenarios from happening.	No change	3.00	
	Security on data transmissions	NA	All data collected through the ECI online collection system is securely transmitted to the data storage so that it cannot be accessed, tampered or destroyed by unauthorised users.	No change	3.00	
	Session management	NA	Users of the ECI online collection system are recognised and kept authenticated for the duration of their transaction, with no possibility of fraudulent reuse by a third party.	No change	3.00	
	Average Score-Security					3.00
	Ease of integration	NA	The solution is integrated seamlessly both in the ECI online collection systems and at Member State level with no additional development effort.	This solution is easy to integrate. Just one module with a simple API is to be integrated. Examples for integration are available.	5.00	
	Maturity	NA	The solution uses proven technologies available on the market.	The solution is mature; all underlying technologies exist on the market since several years.	5.00	
	Portability	NA	The solution can be transferred to different types of device (laptop, tablet, smartphone, etc.) or to different operating systems.	The solution with Java is portable with little effort. Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different application servers. This solution can be used on PCs, tablets and smartphones	5.00	
	Cost/Efforts	NA	The implementation of the solution only requires minor changes in the ECI online collection systems and no change at all at MS level.	This solution can be implemented with a low cost. Estimations are around 3 man-months	5.00	
	Average Score- Integration					5.00

19.6 EVALUATION MATRIX – SOLUTION 6

Solution	Dimension	Evaluation criteria	Domain/Stakeholder	Ideal Example	Description/Justification	Score	
Solution 6: pre-filling data with Facebook	Data Privacy	Data Privacy	NA	The personal data of the user is safely stored.	There is a concern regarding what specific information Facebook would have access to, and where this would be stored, regarding citizens and also organisers of any given initiative. However, information sharing agreements are based on confidentiality obligations that both parties oblige to.	3.00	
	Business Analysis	Ease of Use	NA	The solutions is able to prefill data in a smooth and user friendly way, reducing the time devoted to submit a statement of support.	Retrieving the data from the Facebook account is very simple. Once the user authorised the retrieving of his personal information, the statement of support is automatically prefilled. Then, the user just need to correct it and complete the missing data to comply with the data requirements of each Member State.	3.00	
		Quantity of Data (Input)	NA	The pre-filling solution is able to include a substantial quantity of the data requirements, reducing the fields that the user needs to type in manually	The quantity of data to be input by the user depends on each Member State requirements. The relevant data available on Facebook are: Name, Surname, Date of birth and Address.	2.00	
		Penetration Level/Awareness	NA	The pre-filling solution is based on an account very penetrated at EU level, meaning that a significant amount of citizens across MS will be able to make use of this solution	Facebook has a penetration rate of 39.5% in Europe, meaning that over 307 million people have a Facebook account	3.00	
		Scalability	NA	The solution is able to handle a growing number of MS and signatories without requiring any changes to the architecture of the solution.	No scalability issues exist. New eIDs or new Member States are irrelevant for this solution	5.00	
	Technical Analysis	Maintainability	NA	Any component of the solution can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment without requiring a redesign or refactoring of the system architecture.	No maintainability issues are expected. The specifications of both solutions are not expected to change	5.00	
		Performance & usage of resources	NA	The solution does not impact the performance of the system for the end users and it is able to handle a higher load with an increase of the infrastructure proportional to the total number of users	The CPU usage will increase in an important percentage (around 70%), but the throughput of a modern server is more than enough to support many initiatives in parallel. Performance tests in the STORK project have shown that a modern server can produce and verify some 50 signatures per second, which is 4M signatures per day.	4.00	
		Average Score-Operational Aspects					4.67
		Security on data storage	NA	All data collected through the ECI online collection system is securely stored so that: - it cannot be accessed by unauthorised users; - it cannot be tampered by anybody (EU citizens, ECI organisers, system administrators, etc.), and; - it won't be lost or destroyed.	No change	3.00	
		Fraud prevention	NA	The solution prevents potential fraud scenarios from happening.	No change	3.00	
		Security on data transmissions	NA	All data collected through the ECI online collection system is securely transmitted to the data storage so that it cannot be accessed, tampered or destroyed by unauthorised users.	No change	3.00	
		Session management	NA	Users of the ECI online collection system are recognised and kept authenticated for the duration of their transaction, with no possibility of fraudulent reuse by a third party.	No change	3.00	
		Average Score-Security					3.00
		Ease of integration	NA	The solution is integrated seamlessly both in the ECI online collection systems and at Member State level with no additional development effort.	This solution is easy to integrate. Just one module with a simple API is to be integrated. Examples for integration are available.	5.00	
		Maturity	NA	The solution uses proven technologies available on the market.	The solution is mature; all underlying technologies exist on the market since several years.	5.00	
	Portability	NA	The solution can be transferred to different types of device (laptop, tablet, smartphone, etc.) or to different operating systems.	The solution with Java is portable with little effort. Java can be ported to other operating systems, mostly even without recompiling. It can also be ported to different application servers. This solution can be used on PCs, tablets and smartphones	5.00		
	Cost/Efforts	NA	The implementation of the solution only requires minor changes in the ECI online collection systems and no change at all at MS level.	This solution can be implemented with a low cost. Estimations are around 3 man-months	5.00		
	Average Score- Integration					5.00	

20 APPENDIX I – TERMS AND ACRONYMS

20.1 ACRONYMS USED THROUGHOUT THE REPORT

Acronym	Institution
CA	Certification Authority
CADES	CMS Advanced Electronic Signature
CN	Common Name
CRL	Certificate Revocation List
DIGIT	Directorate-General for Informatics, the European Commission
DN	Distinguished Name
EC	European Commission; the Commission
ECAS	European Commission Authentication Service
ECI	European Citizens' Initiative
eID	Electronic Identification
eIDAS	Electronic Identification and Trust Services (EU Regulation 910/2014)
EU	European Union
e-signature	Electronic Signature
eTS	Electronic Trust Services
ICTs	Information and Communication Technologies
ISO	International Standardization Organisation
IT	Information Technology
LOA	Level of Assurance
MS	Member States
NIST	National Institute for Standards and Technology
OCS	Online Collection System
OID	Object ID
OTP	One-time password
PADES	PDF Advances Electronic Signature
PKI	Public Key Infrastructure
PoC	Proof of Concept
QAA	Quality of Authentication Assurance
SG	Secretariat General of the European Commission
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
XAdES	XML Advanced Electronic Signature

Table 53: Acronyms

20.2 GLOSSARY

Term	Definition
Regulation (EU) 2016/679	Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation)
Commission Implementing Decision (EU)2015/1506	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
Regulation (EU) 910/2014	Regulation (EU) No 910/2014, of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
Regulation (EU) 211/2011	Regulation on the citizens' initiative
Commission Implementing Regulation (EU) 1179/2011	Commission Implementing Regulation (EU) No 1179/2011 of 17 November 2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative.
Directive 1999/93/EC	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
ECI Collection System	Refers to all kind of online collection systems
EC Online Collection System (EC- OCS)	Refers explicitly to the Online Collection System hosted by the European Commission
Man-month	Unit of work representing the productive effort of one person in a 4-week period

Table 54: Glossary