Council of the European Union

Brussels, 3 June 2021
(OR. en)

Interinstitutional File: 2021/0136(COD)

9471/21
ADD 3

TELECOM 242
COMPET 457
MI 432
DATAPROTECT 156
JAI 670
IA 108
CODEC 826

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	3 June 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2021) 124 final PART 2/3
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Annexes Accompanying the document Proposal for a regulation of the European PArliament and of the Council amending Regulation (EU) N° 910/2014 as regards establishing a framework for a European Digital Identity

Delegations will find attached document SWD(2021) 124 final PART 2/3.

Encl.: SWD(2021) 124 final PART 2/3

EUROPEAN
COMMISSION

Brussels, 3.6.2021
SWD(2021) 124 final

PART 2/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Annexes

Accompanying the document

Proposal for a regulation

of the European PArliament and of the Council amending Regulation (EU) N° 910/2014 as regards establishing a framework for a European Digital Identity

{COM(2021) 281 final} - {SEC(2021) 228 final} - {SWD(2021) 125 final}

Table of contents

TABLE OF FIGURES II
ANNEX 1: PROCEDURAL INFORMATION 1
1. Lead, Decide Planning/CWP references 1
2. Organisation and timing 1
3. Consultation of the RSB 1
4. Evidence, sources and quality 8
ANNEX 2: STAKEHOLDER CONSULTATION 9
1. Process and Steps 9
2. Stakeholder feedback Received 10
3. Summary analysis of feedback against policy options 12
4. Open Public Consultation 16
5. Stakeholder Survey 22

Table of figures

Figure 1 - Procedural information - organisation and timing 1
Figure 2 - Actions taken on RSB comments 2
Figure 3 - OPC: Geographical distribution of respondents 16
Figure 4 - OPC: Stakeholders' categories 17
Figure 5 - OPC responses 18
Figure 6 - Stakeholders' views on a European digital identity scheme 20
Figure 7 - OPC: advantages of a European digital identity scheme 21
Figure 8 - OPC: disadvantages of a European digital identity scheme 22
Figure 9 - Stakeholder survey: categories of stakeholders 22
Figure 10 - Stakeholder survey: costs vs benefits related to the adoption of implementing acts referencing standards 23
Figure 11 - Stakeholder survey: cost vs benefits related to introduction of certification requirements 24
Figure 12 - Stakeholder survey: cost vs benefits related to introducing guidelines for the private sector on costing and liability 25
Figure 13 - Stakeholder survey: cost vs benefits related to obligation for MS to provide eID 25
Figure 15 - Stakeholder survey: cost vs benefits related to extension of the current eIDAS framework 27
Figure 16 - Stakeholder survey: cost vs benefits related to a EUeID scheme managed by an EU body 28
Figure 17 - Stakeholder survey: cost vs benefits related to the introduction of an EUeID managed by a consortium 29

ANNEX 1: PROCEDURAL INFORMATION

1. LEAD, DECIDE PLANNING/CWP REFERENCES

The lead DG is the Directorate-General for Communications Networks, Content and Technology. The Decide reference of this initiative is PLAN/2020/8518. The Commission Work Programme for 2021 provides, under the heading ***"A Europe Fit for the Digital Age"***, the policy objective of a trusted and secure European e-ID (legislative, incl. impact assessment, Article 114 TFEU, planned for Q1 2021.

2. ORGANISATION AND TIMING

The Inter-service Steering Group was set up by the Secretariat-General to assist in the preparation of the initiative. The representatives of the following Directorates General were invited to the ISSG: AGRI, BUDG, CLIMA, COMM, COMP, DEFIS, DGT, DIGIT, EAC, ECFIN, EEAS, EMPL, ENER, ENV, ESTAT, FISMA, GROW, HOME, HR, IDEA, INTPA, JUST, JRC, MARE, MOVE, NEAR, OLAF, OP, REFORM, REGIO, RTD, SANTE, TAXUD, TRADE.

Figure 1 - Procedural information - organisation and timing

TIMING	STEP
23 July 2020	Political validation in Decide
23 July 2020	Publication of the Inception Impact Assessments (4-week comment period) and launch of the open public consultation (23 July until 3 September 2020)
7 September 2020	Upstream Meeting with the Regulatory Scrutiny Board
15 December 2020	ISSG Meeting to consult on the draft Impact Assessment
11-15 February 2021	Written consultation of the ISSG
18 February 2021	Submission to RSB
17 March 2021	Consultation of the Regulatory Scrutiny Board
19 March 2021	First (negative) Opinion by the Regulatory Scrutiny Board
5 May 2021	Second (positive) Opinion by the Regulatory Scrutiny Board

3. CONSULTATION OF THE RSB

The meeting of the Regulatory Scrutiny Board ('RSB') took place on 17 March 2021. The outcome was a negative opinion, issued on 19 March 2021. The impact assessment was revised to address the concerns pointed out in the opinion, and in accordance with the improvements

already suggested by DG CNECT in its responses to the checklist that was submitted to the RSB ahead of the meeting. The revised impact assessment was re-submitted to the RSB in April.

The following table provides information on how the comments made by the RSB in its first negative opinion were addressed in this Staff Working Document:

Figure 2 - Actions taken on RSB comments

RSB COMMENTS	ACTIONS TAKEN
Chapter 1 and Chapter 2 • The report should better explain the key problems. • It should draw more clearly on the available evidence from the evaluation to better substantiate the problem definition. • It should clarify the extent to which the problems are related to deficiencies of the existing legislative framework or to implementation issues. • It should elaborate the challenges relating to the new policy context due to the global pandemic, technological change and market developments. • The report should better assess evolving user needs for cross-border eID and trust services, and how far they differ across different use cases (e.g. public services, (semi-regulated sectors, pure private online transactions). • It should better analyse the reasons for the low level of mutual recognition and the limited functionality of currently existing eIDAS nodes. • It should explain related risks and be clearer on where regulatory intervention is warranted as opposed to purely relying on the market.	• Problems and drivers have been redefined in order to strengthen the problem definition and focus on the key problems. The problem tree has been replaced. • The results of the evaluation are summarised in a table format in chapter 1 and referenced in a more systematic way throughout the problem section and complemented by additional information included in Annex 5. • The problem chapter highlights now clearly to what extent the problems are linked to deficiencies of the current framework, its implementation or a change of context. • The challenges due to the new policy context, the global pandemic, technological change and market developments have been elaborated in chapters 1.1, 1.3 and 2.2 (problem drivers). • The report now refers in chapters 1.1, 1.3, and 2.1 to changing user needs for eID and trust services, in particular in relation to attributes and credentials. • The shortcomings identified in relation to eID, in particular the low level of notifications, limitations of the mutual recognition obligation and to the functionality of the eIDAS infrastructure are further explained in the introduction chapter and in the description of the problems and drivers

	(with additional data from the evaluation in Annex 5). • The explanation of the risks and shortcomings of not addressing the identified problems by regulatory intervention is presented in the description of the problems and drivers. • The explanation of the extent to which the future proposal would address concrete problems related to Internet of things and IoT devices is provided in driver 4 and in chapter 5.2.
Chapter 5 – Baseline • The baseline should be further elaborated. • It should explain better how the policy area would evolve without the adoption of the new initiative, taking into account the likely further uptake of trust services and eID schemes. • It should include further implementing measures, standardisation activities and measures already envisaged in the context of other legislative initiatives such as the Digital Market Act. • In addition, it should give a better outlook of the development of alternative market based solutions.	• The baseline is complemented with measures that could be taken under the current framework without legislative change to the eIDAS Regulation. This would include non-adopted implemented acts, adopted implementing acts that could be amended, soft-law instruments or positive spill-overs stemming from other pieces of legislation. • Possible standardization activities and the evolution of technologies are considered in the analysis on how the baseline could evolve. • The baseline now better reflects its potential, integrating market-based solutions and provides a more solid basis for a consistent assessment and comparison of options.
Chapter 5 - Options • The logic behind the options (and the sub options) as well as their respective levels of ambition need to be clarified. • Available policy choices should be clearly identified, including those where stakeholders may have	• The options are reconfigured and grouped along separate set of measures reflecting a gradual level of ambition, from low to high ambition intervention. • The interdependencies between options and underlying measures are clarified, in consistency with the revised

different expectations (e.g. on liability, security, mandatory obligations). • Where appropriate, the report should further explore sub-options or variants. • Decisions to keep or discard certain (sub-options should be justified based on evidence. • The report should more clearly explain which measures will be part of this initiative and which ones will be left to future implementing legislation or standards. • It should specify how the eWallet option would work in practice and how it would affect concerned stakeholders.	intervention logic. • Clarifications are brought to express that the intended objectives can be achieved only by a combination of measures under the existing options. • The specific contribution of measures under option 1&2 to the preferred option (Option 3) is outlined. • Under each option it is specified how measures would be enforced: either by amending the current Regulation or via subsequent implementing acts. • The possible role of the Member States as providers of legal identity to their citizens in the development of the wallet is clarified. The functioning of the wallet and relation to stakeholders is clarified. • It is clarified that the identification of IoT devices can be covered by the new trust service as defined under option 2.
Chapter 6 - Impacts • The report should clearly identify the costs of the preferred option. • They should also be clearly summarised in the cost/benefit table in annex. • The assessment should further specify who will be affected and how, and who has to bear the costs. • All relevant dimensions should be covered, including potential "stranded" costs as well as environmental costs.	• Costs of the preferred option have been clarified and summarized in the cost-benefit table. • The assessment now clarifies who will be affected how and by which costs – summary tables for this purpose have been added. • All relevant dimensions including stranded and environmental costs have been considered as appropriate in chapter 6. In detail: • Section 6.1 has been restructured to increase readability and by providing a concise overview of the main impacts per option. An overview table was provided at the end of the section. • A separate Annex was provided with extensive information on the impacts of each measure and stakeholders,

	complementing the overview of impacts in the text of the IA document. • The REFIT table and the tables included in Annex 3 have been restructured and redrafted to align with the BR template and the information in the CBA, as well as to provide a more transparent overview of the main impacts. • Clarifications were provided strengthening the future-proofness of the preferred option. • The impacts of the wallet on the future use of the existing eID schemes and Member States' investments in their national eID infrastructures was clarified (stranded costs). • The analysis on the impacts on citizens and the social impacts were strengthened by adding additional qualitative information. The same goes for the impact of the options on employment. • The section dealing with SME impacts has been integrated with available information on SME uptake. • The manner in which some impacts will materialise has been clarified in the text. • The comment on the employment impact was addressed by amending the text and by including further information in the Annex presenting the model. • Annex 2 has been integrated with more detailed stakeholder feedback on Option 3, linked to the options as described in the Inception Impact Assessment. • Some qualitative information has been added on environmental impacts. • Key points raised by different stakeholder groups were referenced

	across the report.
Chapter 7 – Comparison • The analysis and comparison of the refined options needs to be strengthened, based on clear and coherent assessment criteria. • The considerations leading to the choice of the preferred option need to be made fully transparent.	• The comparison of options has been strengthened and analysed against objectives. • The considerations leading to the choice of the preferred option have been clarified and the preferred option better linked to chapter 7.
Chapter 8 – Preferred Option / General Comment • The report should more clearly present the views of both public and private stakeholders (including users and identification providers) on this initiative. • Given expressed concerns about the lack of flexibility to adapt to technological developments and changing user needs, the report should better explain how future-proof the preferred option is. • The report should also specify how timely and effective implementation will be ensured given the complexity of the envisaged solution.	• Further stakeholder views have been integrated into the main text where appropriate. The stakeholder annex (annex 2) has been strengthened. • A new extensive annex 5 has been added proving details on all chapters of the IA. The annex has been complemented with further evidence and explanations have been added on the data collection process, particularly in relation to Option 3. • Comments on future-proofness have been added and the implementation scenario has been clarified.
General Comment • The report should have a clear narrative. The main report, in particular the impact analysis, should be shortened by focusing on the most important elements. More technical issues and detailed analyses should be presented in the annexes.	• The overall narrative of the report has been revised, streamlined and strengthened. The report now focuses on the key problems and drivers and the options including the baseline have been restructured. Technical elements and details have been moved into annexes.

The Regulatory Scrutiny Board issued a second positive opinion with comments on the resubmitted draft impact assessment report on 5th May 2021. The following table provides

information on how the comments made by the RSB in its second positive opinion were addressed in this Staff Working Document:

RSB COMMENTS	ACTIONS TAKEN
• (1) The baseline could include a more complete overview of the evolution of the problems, their drivers and some broader impacts (economic, social, technological, environmental and other) if the EU regulatory set-up for electronic identification and trust services remains unchanged. The baseline scenario presented in the impact section should be integrated in the main baseline in the options section.	• As pointed by the Board, the baseline was complemented with additional dimensions linked to possible developments in the absence of legislative intervention; • Stronger emphasis was put on the impact of technological developments and the capacity of the private eID solutions to satisfy evolving needs in the context of the current legislative framework; • The impacts of the scenario where all Member States notify were further substantiated; • Relevant elements previously addressed in the impacts of the baseline scenario (Chapter 6) were integrated accordingly under baseline; • Relevant stakeholders' feedback was integrated;
• (2) Despite a better overall description of options and of the accompanying measures, the report should better explain to what extent policy choices exist on the design and in the combination of measures for each of the options. The report should further clarify the measures' taxonomy, ensuring a consistent approach as to how these are referenced throughout the analysis.	•
• 3) The summary table in the comparison section should provide a more comprehensive overview of the three options' costs and benefits and how they compare in terms of efficiency and effectiveness. The current reference to efficiency does	• A table on the wider impacts per policy option has been added (Figure 23) and a paragraph explaining the relationship between the comparison in Figure 21 with the underlying data • The efficiency section has been updates, providing additional

not sufficiently present the magnitude of actual costs and benefits of each option, including broader societal impacts. As for effectiveness, the narrative of the report could better show the difference in the level of attainment of the specific objectives across all options. The references for the estimates of costs and benefits should also be included to be able to verify the scores.	quantitative elements and an order of magnitude of the overall efficiency gains. • As for effectiveness, text have also been added to the comparison of the options under each objective.
• (4) While more information on stakeholder groups' views are now provided in the annex, the report should present their different positions on the problems, the options and measures more systematically throughout the main text.	• The views of the different stakeholder groups have been included where relevant in the main text of the impact assessment report

4. EVIDENCE, SOURCES AND QUALITY

The Commission has collected feedback from a large number of stakeholders both in the context of the formal meetings with the Member States working groups (e.g. eIDAS Cooperation Network meetings) and in targeted bilateral meetings held with various private and public stakeholders (for details, please see ANNEX 2).

In addition to above actions, the Commission also collected evidence via an open public consultation, desk research, expert interviews, focus groups and workshops with representatives of national authorities of Member States (eIDAS Cooperation Network).

The impact assessment relied on available research in the field of eID and trust services (e.g. studies drafted by ENISA or from other external sources) as well as on statistics, mainly from Eurostat.

The impact assessment was also supported by a study to support the impact assessment for the Digital Identity Act (final report due by 28th February 2020) implemented by a consortium led by PwC and on also a study on the evaluation of the eIDAS Regulation lead by Deloitte.

ANNEX 2: STAKEHOLDER CONSULTATION

1. PROCESS AND STEPS

The Commission engaged in extensive consultation activities with the relevant stakeholders, both during the Open Public Consultation (OPC), in the context of the related call for feedback on the Inception Impact Assessment and similarly after the closure of the formal consultation period, as follows:

- Open Public Consultation (24 July 2020 - 02 October 2020): 318 stakeholders replied, by filling in the questionnaire and, in some cases, also submitting position papers (for the detailed analysis see Annex E of the support study);
- Feedback on the Inception Impact Assessment: Written contributions were submitted by public and private stakeholders (23 July 2020 - 03 September 2020);
- Stakeholder Survey: 106 responses were received (for the detailed analysis see page 209 of the supporting study);
- Survey of Member State representatives of the eIDAS Cooperation Network in July-August 2020 (for detailed results see support study);
- Member States' views expressed during meetings of the eIDAS Cooperation Network (in particular during a dedicated workshop held on 15.01.2021);
- Bilateral meetings with Member States on the revision of eIDAS;
- Presentations by the Commission in the context of 2 Telecom Council Working Groups (June and October 2020);
- Bilateral meetings with various industry stakeholders since spring 2020[1];
- In-depth interviews with 36 public and industry stakeholders from four key sectors with significant customer identification needs and/or regulatory obligations (details provided in Annex E and Annex F of the supporting study).
- 25 in-depth interviews with business stakeholders from the eCommerce, health, Financial services, aviation sector;
- 6 in-depth interviews with subject matter experts of the eID market.

Given the evolution of Option 3 during the preparation process, stakeholder feedback on the final shape of option 3 could only be collected recently and is therefore more limited. As a result, additional effort was made to reduce the gap in evidence compared with other options. The Commission proactively engaged with the Telecom Council Working Group presenting regularly the evolution of the concept. In parallel, the study team carried out additional desk research and targeted interviews focussing specifically on Option 3 (incorporated in the overall count provided above).

The following sections provide an analytical summary of the inputs, while more detailed information is available in the annexes to the study.

[1] E.g. meetings with the European Signature Dialogue, Facebook, Secure Identity Alliance, Infineon, Qualcomm, Eurosmart, Adobe, Yoti, SisuID, Fido, Thales Group, Infocert, and others.

2. STAKEHOLDER FEEDBACK RECEIVED

The current section focuses on the feedback received from public and private stakeholders after the closure of the formal consultation activities (2 October 2020).

Member States:

The feedback received from Member States demonstrated large consensus on the following:

- The need to reinforce the current eIDAS regulatory framework, as described under option 1, and its particular potential to support the other options development. The measure on the harmonisation of certain aspects of the eIDAS Regulation via the use of secondary legislation (i.e. implementing acts) received substantial support, as reflected for intance, in the position put forward by the Forum of European Supervisory Trust Authorities (FESA)[2]. The same goes for the measures aiming to streamline the peer-review and notification processes as incentives and facilitators for further notifications.
- The current minimum dataset is widely perceived by the Member States as too limited. The measures aiming to extend the list of attributes beyond the minimum required dataset and on the private sector re-use of notified eID schemes showed large support.
- The need to establish a trust service allowing the widespread use of attributes in the private sector, a trust service for the identification for non-human entities.
- The introduction of a Digital Identity European framework found support among Member States with universal acceptance and user convenience seen as the most relevant potential advantages. Similarly, Member States agreed on the importance to enable in the future digital identity framework citizens' and companies' possbilities to manage access to both public and private services.

In bilateral exchanges, Member States also highlighted the following:

- Digital identity in Europe should remain anchored in the national registries and eIDs of Member States to provide trust and security. Member States should maintain their role to issue identities of citizens, including in the digital world.
- The need to build a European Digital Identity framework on the experience and strengths of the eID systems developed by the Member States. Complementarity, synergy and capitalizing on the investments made should be the guiding principles when developing the future European eID framework.
- Swift action is needed for eIDAS to reach its full potential and to evolve towards an EU-wide framework for secure public electronic identification enabling control over online identity and data as well as to enable access to public, private and cross-border digital services.

[2] "Harmonization in conformity assessment of Qualified Trust Services (QTSs) is essential for building actual trust in trust services and for mutual recognition of trust services. Harmonization of accreditation and Conformity Assessment Reports (CARs) will allow fair competition between the CABs and will reduce the incentive for QTSPs aiming at the lowest price. Clear and transparent accreditation and certification schemes will foster the uptake and global reach of the eIDAS Regulation. The credibility of conformity assessments and the quality of the CARs will enhance adoption of harmonized accreditation and certification schemes. It will enable TSPs to better make a weighed choice in selecting a CAB without having to make concessions on the quality of the CARs. "

- The eID and trust services frameworks need to be reinforced in order to accelerate the digital transition and to adapt to a fundamentally changed global digital context. This is particularly relevant in the context of the ongoing public health and economic challenges brought about by the COVID-19 pandemic, where eIDs and trust services could act as key drivers for the so much needed economic recovery.
- COVID-19 pandemic has demonstrated, in particular, the value of secure remote identification for all citizens to access essential everyday public and private services, which requires harmonized conditions to be an enabler all across the EU.
- Changes in technology, the dynamics and structure of the identity markets, the increasing role of online platforms acting as identity providers, all these have changed European citizens' expectations on eID. Member States need to respond to these trends and should work towards a solution aiming to both tackle these challenges and to make digital identity a true enabler for business in the Digital Single Market.
- Agreement between Member States on the results of the eIDAS evaluation showing that a strong push is needed to accelerate the pace of notifications under eIDAS (covering currently only about half of the EU population) and on the need to remove the current limitations to the use of eIDs which have an extremely limited reach in the private sector.
- On trust services, the eIDAS Regulation has achieved a lot – has been able to provide a common legal framework, reduced fragmentation of the market and introduced EU-wide interoperability of the solutions. Compared to the situation before eIDAS this is a great achievement.
- However, there are also issues where corrective action is needed. This relates to availability and take-up of services, the comparability of security levels across countries and the harmonisation of supervisory activities.

Stakeholders:

- Most of the stakeholders pleaded for a future digital identity framework which would enables seamless interaction between the primary identities developed by the Member States and the related identity attributes framework needed in a wide set of private use-cases[3].
- A drawback of the current system generally mentioned by the private sector interlocutors was that the use of attributes in the private-sector is currently not enabled under eIDAS.
- Digital identities based on wallets stored securely on mobile devices were highlighted as main recommendation for a future-proof solution. Both the private market (e.g. Apple, Google, Thales) and governments[4] (Germany, United Kingdom[5]) move already in this direction.

---

[3] Views shared by ERSTE Group: *« We believe a common scheme would provide an invaluable strengthening of the use and deployment of electronic identity. A fully harmonized eID scheme in the EU would move from the currently very different schemes toward one common standard which would significantly contribute towards adoption both from a purely technical and economic perspective, but also increase the adoption in terms of ease of acceptance and usage. We believe this should be developed through a public-private partnership. This would enable market competition to take effect and result in a situation similar to the payment industry. »*

[4] Google, Apple, Thales: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/digital-id-wallet

[5] Optioms project in Germany: https://www.bundesdruckerei.de/en/innovations/optimos, UK: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework

- Digital identity wallets are perceived more and more by the private sector as the most appropriate instrument allowing users to choose when and with what private service provider to share various attributes, depending on the use case and the security needed for the respective transaction. The need for a digital identity and attributes trust and interoperability framework was strongly emphasized, based on a clear set of rules, standards, guidelines and best practices which all actors involved agree to follow.
- There is a need for of harmonisation, standardisation and for adoption of guidelines to support greater legal coherence and consistency of the eIDAS framework. The issue of harmonisation is particularly important to trust service and identity providers and should be one of the main corrective actions that must be taken to improve eIDAS.
- The introduction of new trust services for the provision attributes is widely seen by the private sector stakeholders as essential to multiply use-cases and to enable adoption at scale of attributes by the citizens and companies when transacting online

Additional information on stakeholder feedback can be found in Annex of the study to support the impact assessment for the revision of the eIDAS Regulation.

3. SUMMARY ANALYSIS OF FEEDBACK AGAINST POLICY OPTIONS

Feedback on the current policy options can be summarized as follows:

Policy Option 1:

The measure aiming at "enhancing clarity by providing guidance in relation to the LoAs required for specific types of online services" (one of the provisions included in Policy option 1 measure 2) was considered as viable by the majority of respondents to the Cooperation Network Survey. Harmonization of the understanding regarding the use cases between Member States and more guidance to distinguish LoA would facilitate harmonization of requirements and practices. Clear guidance is always welcome. Moreover, one-off adjustment would be limited; **56% of respondents** to the Deloitte / PwC Survey[6] also estimate that benefits would outweigh the costs.

The Open Public Consultation indicates that **43% of the total respondents** selected *standardization and the introduction of certification to the advantage of particularly convenient and secure solutions"* among the needed corrective action to be taken. On the issue of establishing EU-wide certification of security requirements, however, several members of the Cooperation Network thought that the implementation of this policy may involve significant one-off adjustment costs, as well as some recurrent costs per year to consider.

Results from the Deloitte / PwC Survey also show that according to **79% of respondents**, the *adoption of implementing acts referencing standards and adoption of targeted guidelines on the application of specific provisions*) would bring important benefits compared to implementation costs. Clear, more harmonized rules and more transparent regulations across Europe mean less trouble in the certification process and cost savings.

Concerning the *possible extension of the list of attributes covered by Implementing Regulation 2015/1501*, the respondents to the Cooperation Network Survey indicated that costs would be limited to standardisation work. In this respect, it was highlighted that an extension of the list of

[6] See detailed results: Study to Support the Impact Assessment for the Revision of the EIDAS regulation, page 196 ff.

attributes is already considered by the eIDAS technical subgroup and will thus not lead to high additional cost; at the same time, based on this experience, some recognised that it might be challenging to reach an agreement on how to standardise the additional attributes. Some costs may arise from the integration of the existing data sources and connection to the eID node, but the estimate would depend on the range and type of attributes covered by the extension. **Forty-seven per cent of respondents** to the Deloitte / PwC Survey also argued that the implementation of PO1 M5 would bring greater benefits than costs (ranking as the third preference within the overall survey results).

Stakeholders participating in the interviews commented on various aspects of Option 1. Multiple interviewees flagged support for the measures relating to require Member States to allow the private sector to rely on notified eIDs and to establish a cost-model and liability rules (policy option 1, measures 3 and 4). Interviewees acknowledged that the absence of an obligation and the lack of clarity and homogeneity on access conditions for the notified eIDs were a barrier to private sector uptake.

Support was generally expressed with regard to the extension of the minimum dataset, as interviewees from different sectors noted that the lack of some personal and sector-specific attributes had limited uptake of notified eIDs in the past.

Positive comments were further received on the introduction of EU-wide security certification requirements on a voluntary basis. While they recognised that this would be an additional cost initially, they indicated that simplification and harmonisation would create benefits that outweigh this initial cost. They also indicated, however, that one risk with certification may arise when requirements fall behind technological developments, and therefore it should be ensured that these requirements are reviewed periodically.

In the interviews, there was also general consensus on the necessity of greater harmonisation of supervisory procedures for Trust Services, which more than one interview considered as long due.

Policy Option 2:

The OPC suggests significant stakeholder interest in PO2 M1, which encompasses the *introduction of new private sector digital identity trust services for identification, authentication and provision of attributes* (41%) and the *provision of identification for non-human entities* (20%). Further, 41% of respondents to the Deloitte / PwC survey were positive towards measures to strengthen data protection and privacy, (PO2 M6) perceiving their benefits as greater than their cost.

Interviewees provided general perspectives on the notion of extending the scope of the Regulation to the private sector, including by creating a new trust services covering the provision of attributes (which is most relevant to policy option 2, measure 1: Creating a new Qualified Trust Service for the secure exchange of data linked to identity). The stakeholders generally welcomed the idea, noting that a comprehensive legal framework for digital identity should take into account private actors, given their increasingly important role in the landscape, and that enhancing the cross-border exchange of attributes related to identity in a secure way would benefit both end users and the service providers. They also noted the market opportunities that may emerge from the possibility of providing credentials, noting however that the choice of business models for providers may not be obvious and would require careful consideration.

In this context, multiple stakeholders also indicated that the regulation of non-human entities (e.g. IoT devices) would be increasingly important because they recognised it as an area where IT security and data privacy need to be strengthened as a matter of priority. For example, one stakeholder noted that these devices generally do not come with guarantees of timely and ongoing software updates and cited research showing that 82% of IT professionals predicted that unsecured IoT devices would cause a data breach — likely significant — within their organisation.

Measures to strengthen the protection of personal data (policy option 2, measure 6) were also generally welcomed, in light of the fact that an extension of the regulation to private actors would require clear and strong safeguards to the privacy of end users.**Policy Option 3:**

The results of the Open Public Consultation indicate that a large majority of respondents **(63%)** would welcome the creation of a single and universally accepted European Digital Identity scheme, complementary to the national publicly issued electronic identities. However, **52% of the respondents** to the Open Public Consultation also indicated the complexity of set-up and Governance of a single and uniform European digital identity scheme as the main possible challenges. The analysis conducted on the results of the three different surveys allows to highlight some aspects that are widely acknowledged by the respondents and which should certainly be addressed:

- **the universal acceptance of eID schemes**: the cross-border acceptance of national digital identity schemes is often highlighted as one of the main shortcomings of current Regulation. In fact, 47% of the total respondents to the Open Public Consultation indicated the universal acceptance of a possible EUeID scheme as the main advantage;
- **enhance clarity and provide targeted guidelines**: corrective actions related to the introduction of guidelines for the private sector, the application of specific provisions, to improve legal coherence and consistency or to provide guidance in relation to the LoAs are always indicated as useful and necessary by respondents. Clear guidance is always welcome;
- **extend the scope of eID regulation under eIDAS to the private sector**: the introduction of obligations and the extension of the eIDAS regulation to the private sector is often remarked by respondents. 49% of respondents to the Open Public Consultation consider it as the main corrective action to be taken at EU level.

In addition, on the notion of creating an EU Digital identity, interviewees generally recognised the potential benefits of an eID means that would be recognised across borders and usable across a wide range of public and private services, with some exceptions. The most positive views were expressed by representatives of service providers with multi-country operations, as these placed a higher value on the benefits of frictionless cross-border use of eIDs. Interviewees from across the financial, eHealth, transport and eCommerce sector could all identify ways that such a scheme could help increase efficiency and improve customer experience in their own sectors, provided that the EU eID could deliver wide uptake and make available all of the required attributes (general and sector-specific) for the relevant use cases.

By contrast, these benefits were recognised to a lesser extent by others with a more national customer base. These stakeholders expressed some doubts over the added value of a European Digital Identity given that most service transactions are made nationally, although they

welcomed the advantages this is expected to bring in terms of security, data protection and user control. The interviewed stakeholders who expressed opposition or concerns about the measure also did so for a number of reasons that were mostly linked to the demanding implementation of the measure or its political feasibility. Interviewees recognised that the scheme could have broad application across a number of sectors (e.g. mobility, education, health, finance, eCommerce) if it allowed users to exchange a wide range of qualified attributes and credentials related to their identity, and welcomed proposals for the scheme to be designed in line with principles of user-centricity, privacy and security. Finally, they saw the required negotiations with mobile manufacturers and network operators for the required access to the SE/eSIM as potentially complex, but viable. Reservations were mainly expressed by interviewees regarding potential complexity of implementation and the uncertain impact on existing business models for eID providers.

4. OPEN PUBLIC CONSULTATION

The Open Public Consultation, distributed online from 24 July to 2 October 2020, aimed to collect feedback on drivers and barriers to the development and uptake of eID and trust services in Europe and on the impacts of the options available to delive an EU digital identity. It targeted broad public (e.g. citizens and end-users, including older persons and persons with disabilities) as well as companies directly impacted by the eIDAS Regulation (e.g. trust service providers, identity providers), competent authorities in the Member States, international organisations and concerned stakeholders on the eIDAS framework.

The Open Public Consultation received responses from a total of 318 stakeholders. The figures below report the overview of the geographical distribution of the countries and the categories to which the respondents belong.

Figure 3 - OPC: Geographical distribution of respondents

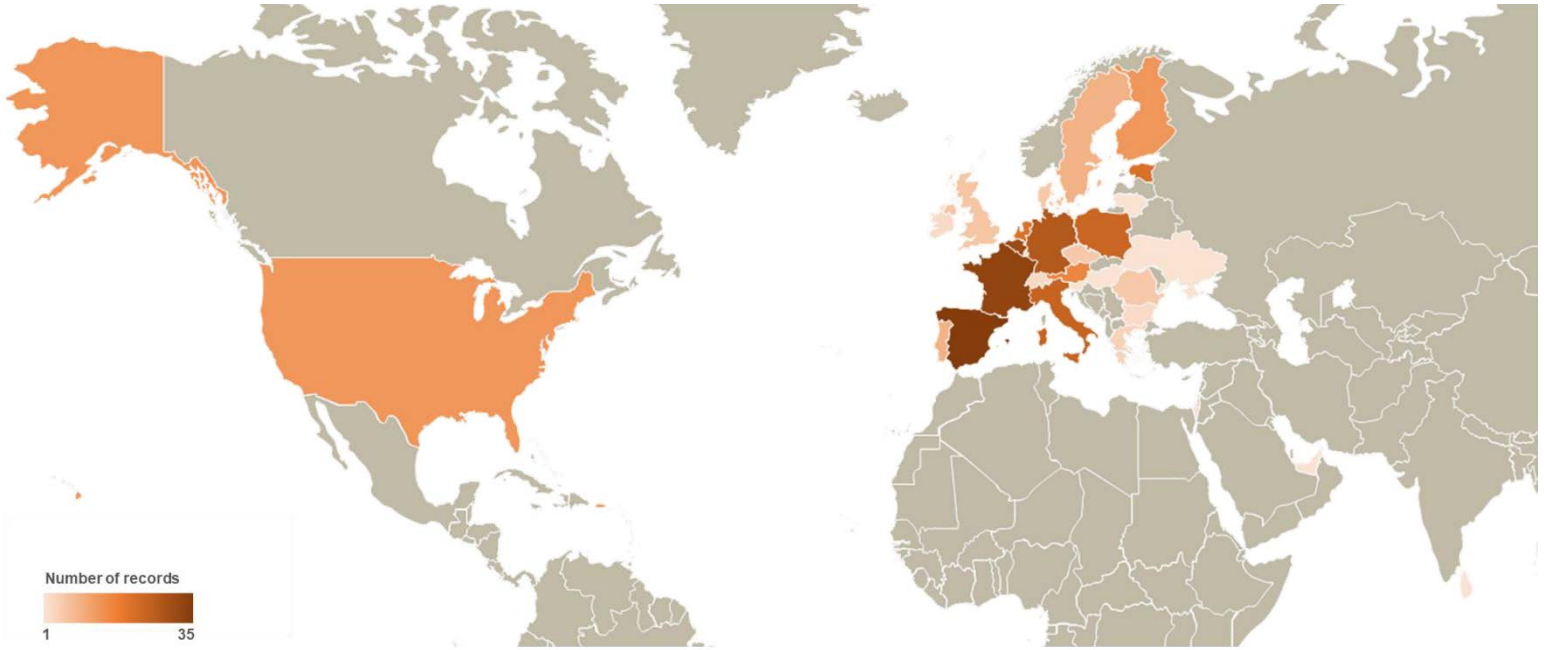
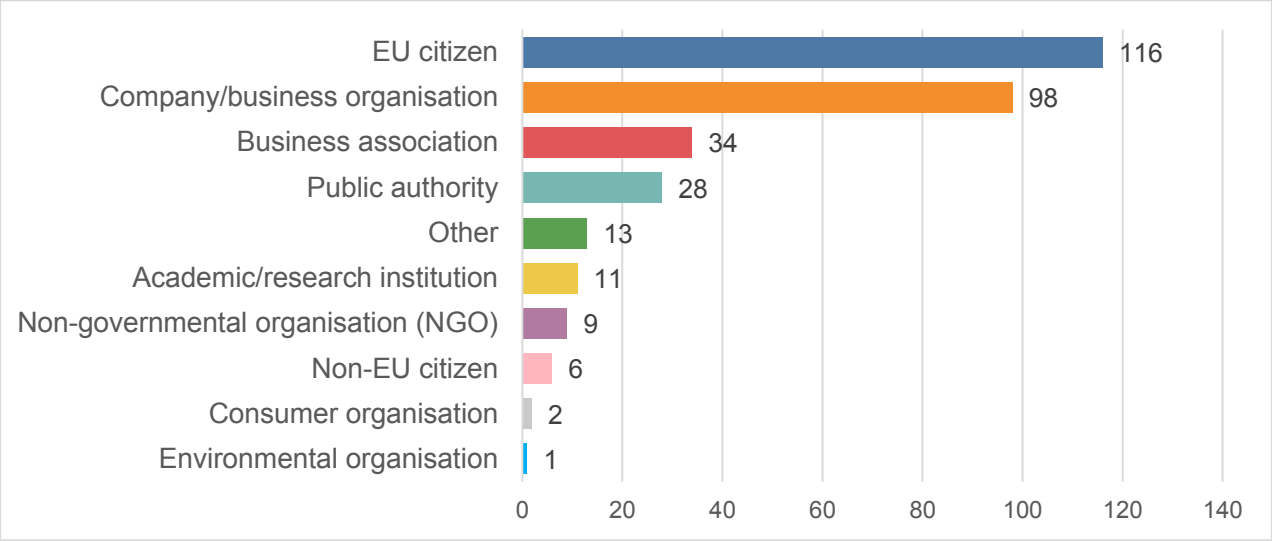


Figure 4 - OPC: Stakeholders' categories

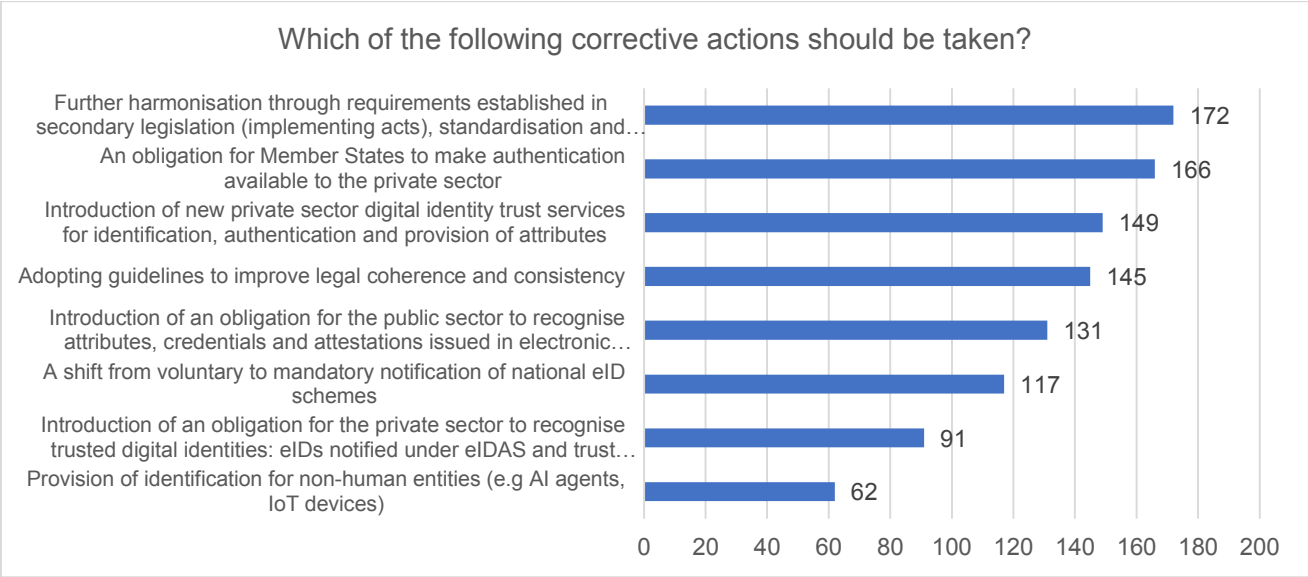


The Study Team contributed to the drafting of the questionnaire by inserting some specific questions useful for the elaboration of the impact assessment for the Digital ID Act. The results obtained are reported in the following paragraphs. The first question was intended to understand which corrective actions should be taken in the context of the revision of eIDAS to try to overcome the shortcomings of the current eIDAS regulation. Respondents had the possibility to choose one or more preferences from the following options:

- adopting guidelines to improve legal coherence and consistency;
- further harmonisation through requirements established in secondary legislation (implementing acts), standardisation and the introduction of certification to the advantage of particularly convenient and secure solutions;
- a shift from voluntary to mandatory notification of national eID schemes;
- an obligation for Member States to make authentication available to the private sector;
- introduction of new private sector digital identity trust services for identification, authentication and provision of attributes;
- introduction of an obligation for the public sector to recognise attributes, credentials and attestations issued in electronic form by trust service providers and public authorities registered as authoritative sources;

- introduction of an obligation for the private sector to recognise trusted digital identities: eIDs notified under eIDAS and trust services for identification, authentication and provision of attributes;

Figure 5 - OPC responses



81 respondents did not provide any answers to this question. The remaining 237 respondents, who provided one or more answers to the question, considering the actions:

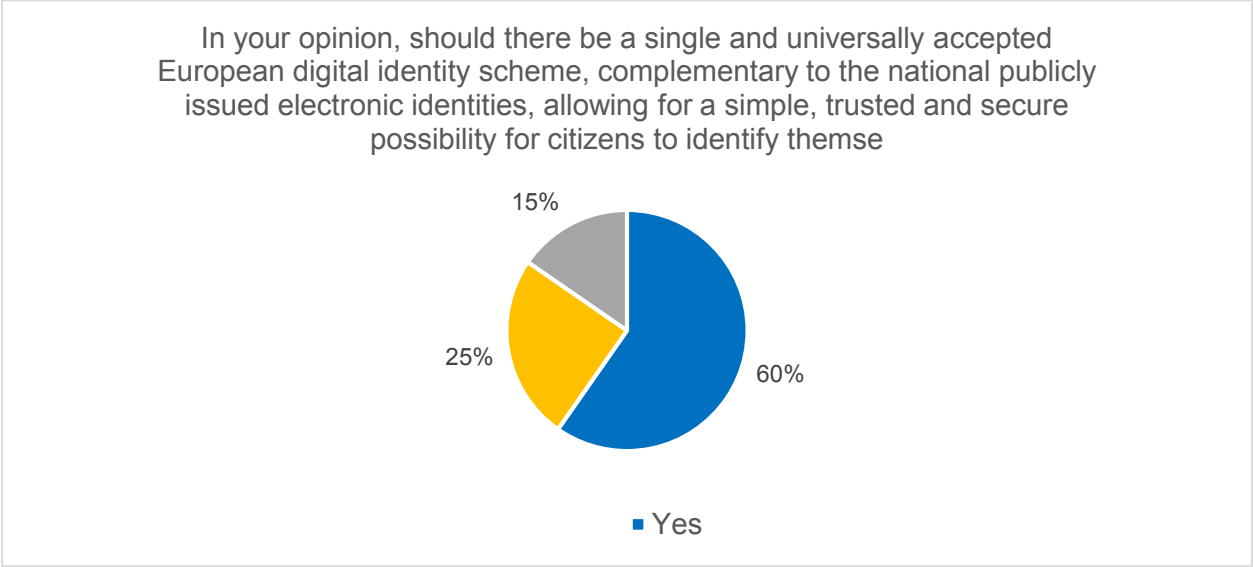
- further harmonisation through requirements established in secondary legislation (implementing acts), standardisation and the introduction of certification to the advantage of particularly convenient and secure solutions;
- an obligation for Member States to make authentication available to the private sector;
- introduction of new private sector digital identity trust services for identification, authentication and provision of attributes,

as the main corrective actions to be taken at EU level to overcome the shortcomings of the current eIDAS regulation. The preferred action, namely "further harmonisation through requirements established in secondary legislation (implementing acts), standardisation and the introduction of certification to the advantage of particularly convenient and secure solutions", received 172 votes, corresponding to **54% of the total respondents**.

As a second preference, the action who received more votes is "**an obligation for Member States to make authentication available to the private sector".** This corrective action was indicated by **52% of the total respondents.**

The second question aimed to understand the possible need to create **a single and universally accepted European digital identity scheme**, **complementary to the national publicly issued electronic identities**, allowing for a simple, trusted and secure possibility for citizens to identify themselves online.

Figure 6 - Stakeholders' views on a European digital identity scheme

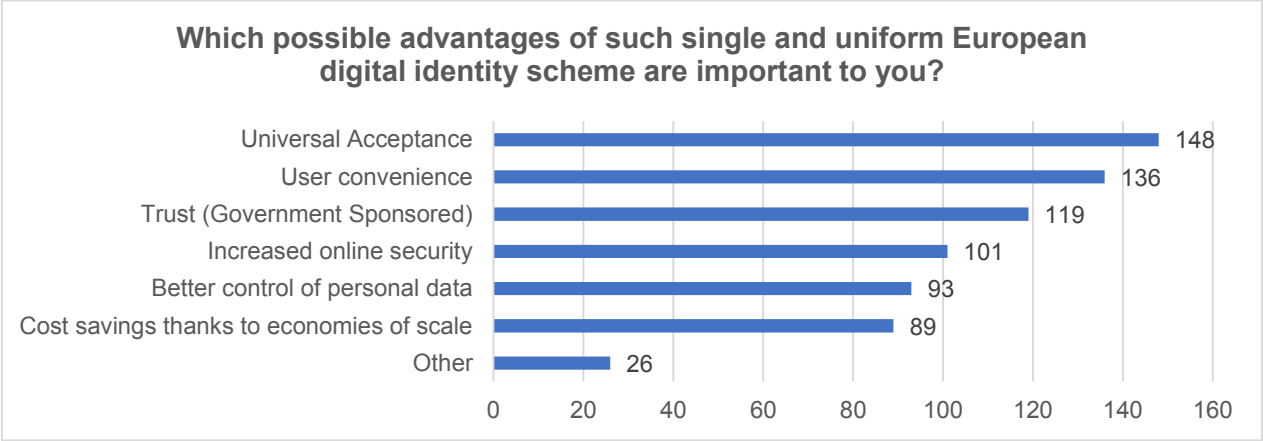


A large majority of respondents (**60%**) would gladly welcome the creation of a single and universally accepted European digital identity scheme, complementary to the national publicly issued electronic identities.

The various participants were also asked which **possible advantages of such single and uniform European digital identity scheme are important** to them. Respondents had the possibility to choose **one or more preferences** from the following options:

- trust (Government Sponsored);
- universal Acceptance;
- user convenience;
- better control of personal data,
- increased online security;
- cost savings thanks to economies of scale;
- other.

Figure 7 - OPC: advantages of a European digital identity scheme



155 respondents did not provide any answers to this question. The main advantage indicated by the remaining participants is the **universal acceptance (148 votes)** that a single and uniform European digital identity scheme could bring to the EU citizens. The universal acceptance has been indicated as the main advantage by **47% of the total respondents**.

As a second and third possible advantage that were indicated by the participants there are:

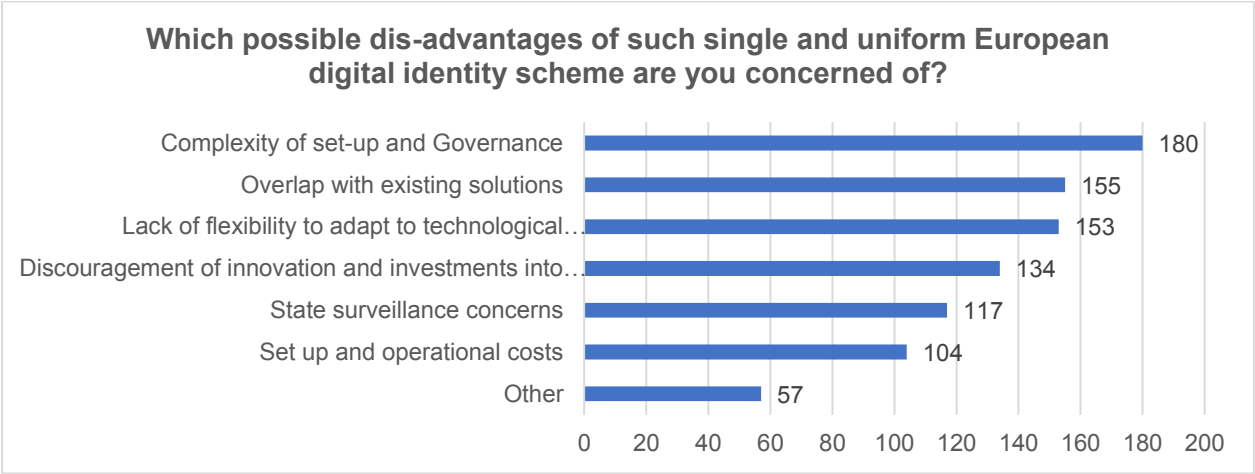
- **user convenience**, voted by **43% of the total respondents;**
- **trust (Government Sponsored),** voted by **37% of the total respondents.**

Participants were also asked to indicate which **possible dis-advantages of such single and uniform European digital identity scheme** are to consider. Respondents had the possibility to choose **one or more preferences** from the following options:

- complexity of set-up and Governance;
- lack of flexibility to adapt to technological developments and changing user needs;
- overlap with existing solutions;
- discouragement of innovation and investments into alternative eID solutions;
- state surveillance concerns;
- set up and operational costs;

- other.

Figure 8 - OPC: disadvantages of a European digital identity scheme



35 respondents did not provide any answers to this question. **57% of the respondents** to the Open Public Consultation indicated the **complexity of set-up and Governance** of a single and uniform European digital identity scheme as the main possible dis-advantage.

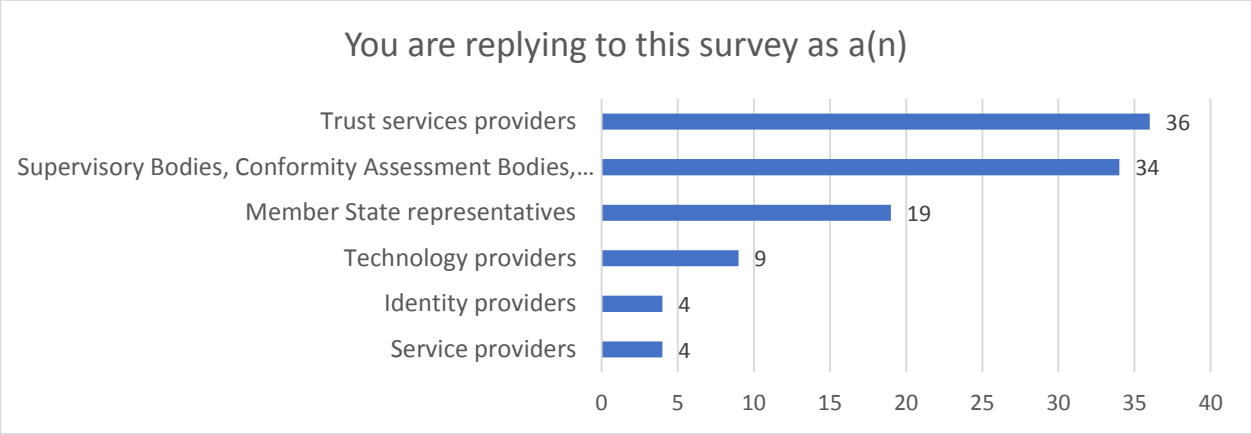
The overlap with existing solutions (**49% of the total respondents**) and the lack of flexibility to adapt to technological developments and changing user needs (**48% of the total respondents**) are also to consider as possible dis-advantages.

5. STAKEHOLDER SURVEY

In the context of the "eIDAS Review", the contractor (PwC) conducting external support study gathered data and information to support the impact assessment for the revision of the eIDAS regulation.

A total of **106 responses** to the survey we received from the following categories of stakeholders:

Figure 9 - Stakeholder survey: categories of stakeholders



Different questions were sent to each stakeholder category based on the most suitable policy options for each specific category.

Policy Option 1

Under this option, a European Digital Identity would be created in the form of a strengthened legislative framework for national eIDs notified under eIDAS, requiring Member States to make eIDs available to all citizens and companies for cross-border use and improve the effectiveness and efficiency of mutual recognition. The use of national eIDs by private online service providers would be triggered and facilitated through harmonised cost and liability rules, extended data sets and access obligations. All these measures would be taken without extending the regulation scope nor affecting its underlying principles (e.g. applicable to eID solutions notified by Member States, mutual recognition and technological neutrality).

Questions about the Policy Option 1 were targeted to the following stakeholders' categories:

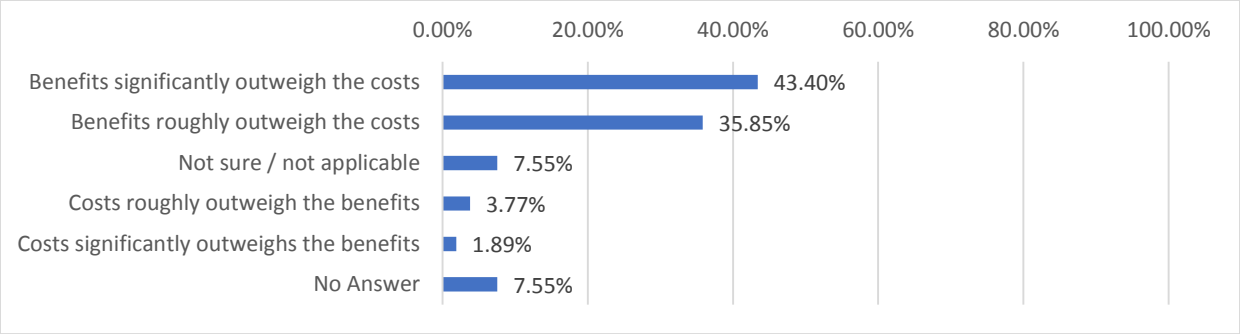
Member State representatives;

Supervisory Bodies, Conformity Assessment Bodies, Accreditation bodies.

Questions asked concerned the following measures:

1.1 Adoption of implementing acts referencing standards (audit schemes, conformity assessment, supervisory authorities) and adoption of targeted guidelines on the application of specific provisions (e.g. remote identification, identity proofing)

Figure 10 - Stakeholder survey: costs vs benefits related to the adoption of implementing acts referencing standards



	Answers	%
Benefits significantly outweigh the costs	23	43,40%
Benefits roughly outweigh the costs	19	35,85%
Not sure / not applicable	4	7,55%
Costs roughly outweigh the benefits	2	3,77%
Costs significantly outweighs the benefits	1	1,89%
No Answer	4	7,55%

The results show how **79,25% of stakeholders** consider that the benefits from the adoption of implementing acts referencing standards and the adoption of targeted guidelines on the application of specific provisions would outweigh the costs.

Replies to this measure with "Benefits significantly outweigh the costs" amounted to **more than 43%** and "Benefits roughly outweigh the costs" a bit lower than **36% of respondents**.

1.2 Introduction of new requirements for the certification of eID means e.g. by referencing European cybersecurity certification schemes in the IA on LoAs.

Figure 11 - Stakeholder survey: cost vs benefits related to introduction of certification requirements

	Answers	Ratio
Benefits significantly outweigh the costs	7	13,21%
Benefits roughly outweigh the costs	10	18,87%

	Answers	Ratio
Not sure / not applicable	20	37,74%
Costs roughly outweigh the benefits	5	9,43%
Costs significantly outweighs the benefits	5	9,43%
No Answer	6	11,32%

The respondents involved are a bit more dubious about the measure above. Thirty-two per cent of respondents indicate that benefits would outweigh the costs while 19% of respondents estimate that costs would outweigh the benefits.

1.3 Introduce guidelines for the private sector on costing, liability and on the opportunities to fulfil various regulatory requirements by the use of eIDs

Figure 12 - Stakeholder survey: cost vs benefits related to introducing guidelines for the private sector on costing and liability

	Answers	Ratio
Benefits significantly outweigh the costs	9	16,98%
Benefits roughly outweigh the costs	16	30,19%
Not sure / not applicable	21	39,62%
Costs roughly outweigh the benefits	1	1,89%
Costs significantly outweighs the benefits	1	1,89%
No Answer	5	9,43%

Considering the measure above, **47% of respondents** estimate that benefits would outweigh the costs. This percentage represents a clear majority compared to **4% of respondents** who estimate that costs would outweigh the benefits.

1.4 Establish Regulatory obligations for Member States to make available to their citizens highly secure and convenient national eID schemes

Figure 13 - Stakeholder survey: cost vs benefits related to obligation for MS to provide eID

	Answers	Ratio
Benefits significantly outweigh the costs	7	13,21%

Benefits roughly outweigh the costs	14	26,42%
Not sure / not applicable	21	39,62%
Costs roughly outweigh the benefits	4	7,55%
Costs significantly outweighs the benefits	2	3,77%
No Answer	5	9,43%

A similar pattern as that recorded for Q 1.3 can be found in the result of the Q 1.4 considering the possibility to establish regulatory obligations for Member States to make available to their citizens highly secure and convenient national eID schemes.

40% of respondents in total consider that benefits outweigh the costs compared to a small percentage of **11% of respondent** who expect costs to exceed benefits.

Policy Option 2

Under this option, the private sector would support the delivery of a European digital identity ecosystem in the form of a new qualified trust service for the exchange of digital identity attributes, such as proof of age (e.g. for accessing age restricted social media), professional qualifications (e.g. lawyer, student, doctor), digital driving licences, vaccination certificates etc. across borders. The scope of eIDAS would be expanded to cover this new trust service. In this new ecosystem, identity data and attributes would, whenever required, be securely linked to the legal eID of the user, making the data trustworthy and legally enforceable across borders. National eIDs notified under eIDAS would continue to be the sole means to provide legal identity across borders when this is required (e.g. for public services, such as submitting a tax declaration online).

	Answers	Ratio
Benefits significantly outweigh the costs	11	12,64%
Benefits roughly outweigh the costs	24	27,59%
Not sure / not applicable	43	49,43%
Costs roughly outweigh the benefits	11	12,64%
Costs significantly outweighs the benefits	8	9,20%
No Answer	9	10,34%

2.1 Focus on protection of data and privacy (establish Obligations on digital services providers to split data between data collected for the purpose of user identification and the provision of the digital ID service, and (2) data generated by the user's subsequent activity on the third party service providers' website, and transparency)

Forty per cent of stakeholders, answering to this question believe that benefits would outweigh the costs. **Only 22% of respondents** do not see significant benefits from implementing this measure.

Policy Option 3

Policy Option 3 would introduce a European Digital Identity scheme (EUid). Questions about this option were asked in summer 2020 as part of the stakehoder surveys, and targeted to the following stakeholders' categories:

- Member State representatives;
- Supervisory Bodies, Conformity Assessment Bodies, Accreditation bodies;
- Identity providers.

It must be borne in mind that the implementation options that were presented in those surveys were different from the ones considered in this impact assessment. Specifically, respondents were asked to comment on the following implementation scenarios:

- Option 3.1 Aggregate existing national eID schemes – extension of the current eIDAS framework (The sub-option will be an evolution of the current eIDAS framework, it implies maximum diversity of eID means and identity providers)
- Option 3.2 Introduction of a new European eID scheme managed by an EU body (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, one single identity provider)
- Option 3.3 Introduction of a new European eID scheme managed by a consortium / association (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, several identity providers (at least one per MS)

The results recorded for Policy Option 3 show more clearly how the various stakeholders involved are not convinced about the benefits or applicability of these three sub-options. As noted above, however, these results may not be representative of stakeholder opinions on an EU eID Wallet App as presented in this impact assessment, since their comments were based on different implementation options and significantly less implementation detail on the proposals for an EU eID.

3.1. Aggregate existing national eID schemes – extension of the current eIDAS framework (The sub-option will be an evolution of the current eIDAS framework, it implies maximum diversity of eID means and identity providers)

Figure 15 - Stakeholder survey: cost vs benefits related to extension of the current eIDAS framework

	Answers	Ratio
Benefits significantly outweigh the costs	11	19,30%
Benefits roughly outweigh the costs	13	22,81%
Not sure / not applicable	21	36,84%
Costs roughly outweigh the benefits	1	1,75%
Costs significantly outweighs the benefits	5	8,77%
No Answer	6	10,53%

The option Q 3.1 is the only one of the three considered in this section in which the various stakeholders are more in favour of adopting the policy than against: 42,11% of respondents estimate that benefits would outweigh the costs and 10,52% of respondents think opposite.

3.2. Introduction of a new European eID scheme managed by an EU body (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, one single identity provider)

	Answers	Ratio
Benefits significantly outweigh the costs	8	14,04%
Benefits roughly outweigh the costs	5	8,77%
Not sure / not applicable	21	36,84%
Costs roughly outweigh the benefits	11	19,30%
Costs significantly outweighs the benefits	6	10,53%
No Answer	6	10,53%

Figure 16 - Stakeholder survey: cost vs benefits related to a EUeID scheme managed by an EU body

In this case the respondents are not in favour of applying the measure: **29,82% of respondents** estimate that costs would outweigh the benefits compared to **22,81% of respondents** who argue otherwise.

3.3 Introduction of a new European eID scheme managed by a consortium / association (The sub-option will be separated from the current eIDAS framework, it implies limited diversity of eID means, several identity providers (at least one per MS)

Figure 17 - Stakeholder survey: cost vs benefits related to the introduction of an EUeID managed by a consortium

	Answers	Ratio
Benefits significantly outweigh the costs	3	5,26%
Benefits roughly outweigh the costs	5	8,77%
Not sure / not applicable	29	50,88%
Costs roughly outweigh the benefits	5	8,77%
Costs significantly outweighs the benefits	9	15,79%
No Answer	6	10,53%

The last option shows an even sharper orientation than the previous one: **24,56% of respondents** estimate that the measure would involve more costs than achievable benefits compared to **14,04% of respondents** who see benefits achievable from the application of the policy option.