



Brussels, 3.6.2021
SWD(2021) 130 final

EVALUATION

COMMISSION STAFF WORKING DOCUMENT *Accompanying the document*

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

**on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust
services for electronic transactions in the internal market (eIDAS)**

{COM(2021) 290 final} - {SEC(2021) 229 final}

Table of contents

1. INTRODUCTION	5
2. BACKGROUND	5
Description of the intervention and its objectives	5
Baseline and points of comparison.....	7
3. IMPLEMENTATION / STATE OF PLAY	11
Electronic identification	11
Trust services.....	14
4. METHOD.....	17
5. ANALYSIS AND ANSWERS TO THE EVALUATION QUESTIONS	19
5.1 Effectiveness	19
Q1. To what extent has the Regulation met its operational objectives?.....	20
Q2. To what extent has the Regulation met its specific objectives?	29
Q3. To what extent has the Regulation met its general objectives?	33
5.2 Efficiency	35
Q4. Did the regulatory intervention create any additional costs and benefits for targeted stakeholders?	35
Q5. How proportionate is the amount of costs and benefits to cost and benefit items? How are they broken down? How do they compare across different stakeholder groups?	40
Q6. To what extent have the aggregate costs of the Regulation been justified and proportionate given the aggregate benefits achieved?.....	44
Q7. Are there opportunities to simplify the legislation or reduce unnecessary regulatory costs without undermining the intended objectives of the intervention?	46
5.3 Relevance	47
Q8. To what extent do the initial objectives still correspond to the current needs and concerns?	47
Q9. To what extent do the solutions and standards address user needs?.....	49
Q10. To what extent are there adaptation mechanisms in place to follow technological, scientific and social developments?	51
Q11. To what extent has the eIDAS Regulation addressed relevant needs in specific sectors and what other areas should be covered?	52
Q12. To what extent have alternative solutions been developed to address current needs, in parallel with the mechanisms and solutions foreseen by the eIDAS Regulation?	55
Q13. How does the eIDAS Regulation support the requirements for customer data portability and the emerging paradigm of full user control of personal data (as proposed by MyData or the Decentralised Identity Foundation)?	56

Q14. How well adapted is the intervention to subsequent technological or scientific advances? What are the opportunities for expanding the number of trust services currently covered by the Regulation (by e.g. blockchain, eArchiving, IoT) and for extending eID services to the private sector?	58
5.4 Coherence.....	60
Q15. Are there issues of internal coherence (i.e. between parts of the eIDAS Regulation and implementing acts)?	60
Q16. Are there coherence issues with relevant Member States' rules and regulations?	67
Q17. Are there overlaps or complementarities between the eIDAS Regulation and any other Community actions, which share objectives?	69
5.5 EU added value	76
Q18. Is there additional value (at national, European and international level) resulting from the eIDAS Regulation, compared to what could be achieved with similar regulatory frameworks at national level?.....	76
Q19. To what extent do the issues addressed by the eIDAS Regulation require further action at EU level? Which recommendations can be made to improve EU added value?.....	76
Q20. What would be the most likely consequences of repealing the eIDAS Regulation?.....	77
6. CONCLUSIONS.....	77
ANNEX 1: PROCEDURAL INFORMATION	84
ANNEX 2: STAKEHOLDER CONSULTATION	87
ANNEX 3: METHODS USED IN PREPARING THE EVALUATION	99
ANNEX 4: ADDITIONAL INFORMATION	116

GLOSSARY

<i>Term or acronym</i>	<i>Meaning or definition</i>
BYOI	Bring your own identity
eIDAS	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market
eID	Electronic Identification
ENISA	European Union Agency for Cybersecurity
ERDS	Electronic Registered Delivery Service
ETSI	European Telecommunications Standards Institute
FATF	Financial Action Task Force
FESA	Forum of European Supervisory Authorities for trust service providers
GDPR	General Data Protection Regulation
KYC	Know Your Customer
LEI	Legal Entity Identifier
LoA	Level Of Assurance
LOTL	European List of Trusted Lists
NFC	Near-field communication
NQTS / QTS	Non-Qualified Trust Service / Qualified Trust Service

NQTSP / QTSP	Non-Qualified Trust Service Provider / Qualified Trust Service Provider
OOP	Once Only Principle
PKI	Public key infrastructure
PSD	Payment Services Directive
QWAC	Qualified Website Authentication Service
SDGR	Single Digital Gateway Regulation
TSPs	Trust Service Providers
W3C	World Wide Web Consortium

1. INTRODUCTION

Article 49 of Regulation EC 910 (2014) on electronic identification and trust services for electronic transactions in the internal market (hereafter “the eIDAS Regulation”)¹ requires the Commission to review the application of this Regulation and to evaluate in particular whether it is appropriate to modify its scope or its specific provisions taking into account the experience gained in its application, as well as technological, market and legal developments.² This Staff Working Document (SWD) provides the results of the evaluation of the application of the eIDAS Regulation. The Commission has assessed to what extent the eIDAS framework remains fit for purpose delivering the intended outcomes, results and impacts. In addition, the evaluation also identifies areas where the current digital identity and trust services framework can be improved or complemented.

The evaluation provides critical assessment of the implementation of the legal framework and its adoption at EU and Member State level including its implementing acts and the sectoral legislation that refer to the eIDAS framework³. It identifies possible gaps, opportunities and challenges, as well as potential gains in efficiency, effectiveness, and regulatory simplification and formulates conclusions and recommendations where applicable.

The evaluation covers EU Member States and EFTA EEA countries (Iceland, Liechtenstein and Norway) including the period of membership of the United Kingdom. Cooperation with 3rd countries is also assessed where appropriate.

2. BACKGROUND

Description of the intervention and its objectives

The eIDAS Regulation was adopted by the European Parliament and the Council on 23 July 2014 and entered into force on 28 July 2014.⁴ The Regulation was conceived as an instrument to ensure the proper functioning of the internal market and an adequate level of security of electronic identification means and trust services. The objective of the eIDAS Regulation is to enhance trust in electronic transactions in the internal market by providing a common foundation for secure and seamless electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the EU. It repeals Directive [1999/93/EC](#) on a Community framework for electronic signatures.

¹ Regulation 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 and repealing Directive 1999/93/EC, *OJ L 257*, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>.

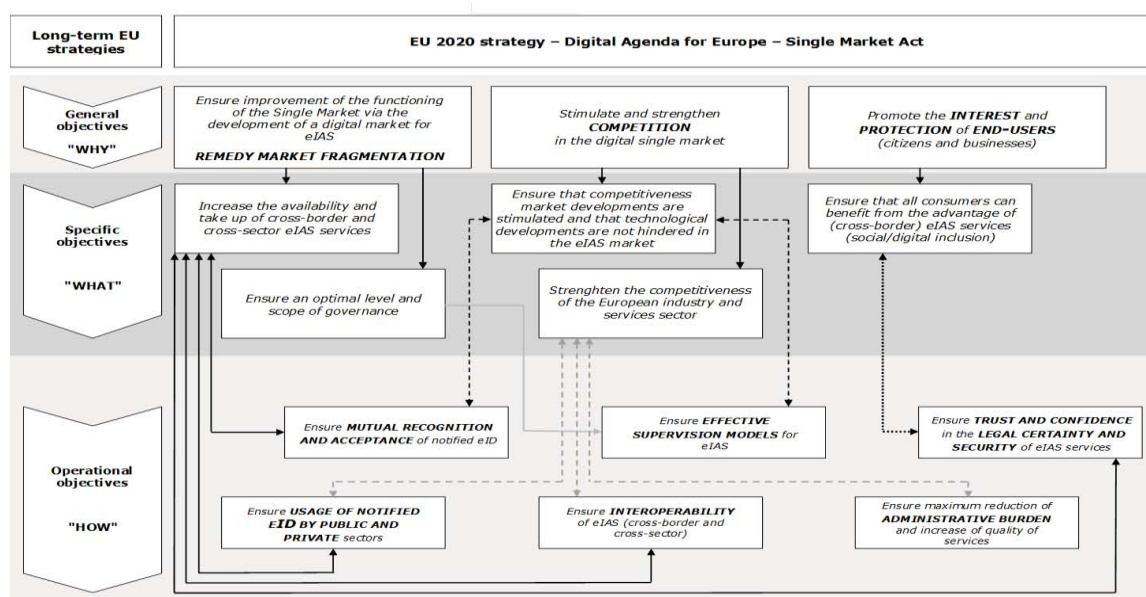
² “The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments.”

³ Such as regulation in the area of online banking, eCommerce, transport, login to websites, safer internet services, audio-visual services, eGovernment and Company law.

⁴ A series of provisions entered into force later: On 17 September 2014 entered into force articles conferring powers to the European Commission to adopt delegated and implementing acts, on 1 July 2016 entered into force provisions linked to the introduction of a common regulatory framework for trust services and from 29 September 2018 entered into force provisions linked to the mutual recognition of notified eID schemes.

The figure below provides an overview of the general objectives of the Regulation as well as the specific and operational objectives as described in the initial impact assessment supporting the adoption of the regulatory framework.

Figure 1: Overview of general, specific and operational measures of the eIDAS Regulation⁵



The key challenges the eIDAS Regulation seeks to address are fragmentation in the market for eID and trust services and a lack of trust and confidence in electronic transactions. Further to its legal base, Article 114 TFEU, the eIDAS Regulation intends to improve the functioning of the Digital Single Market by increasing the availability and take-up of electronic identification and trust services cross-border and cross-sector and by stimulating and strengthening competition.

For this purpose, the eIDAS Regulation introduces a predictable and comprehensive legislative framework to enable secure and trustworthy electronic transactions between businesses, citizens and public authorities. More specifically, the eIDAS Regulation seeks to:

- ensure that individuals and businesses can use their national **electronic identification** schemes (**eIDs**) for online access to public services in other EU Member States through establishing interoperability and enforcing mutual recognition.
- create a European internal market for **electronic Trust Services (eTS)** - namely electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication - by ensuring that they are recognised across borders with the same legal status as traditional paper based processes. The main aim of the eIDAS Regulation in this respect is to foster transparency and trust in online services as a means of stimulating the internal market.

One of the cornerstones of the Regulation is the **risk-based approach**. For trust services, the eIDAS framework imposes certain specific risk management and security obligations on qualified trust service providers and establishes a clear liability regime to ensure compliance at various levels. The risk management approach covers operations, conduct and procedures. For eID, cooperation among Member States should facilitate technical interoperability of notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the

⁵ Source: SWD(2012) 135 final, page 23.

degree of risk. Exchange of information and sharing of best practices facilitates mutual recognition and cooperation.

The eIDAS framework follows an **outcome-based approach**. Based on the principle of technological neutrality, it establishes minimum requirements, standards and procedures to achieve the necessary security requirements.⁶

Mutual recognition of eID systems only applies to those electronic identification schemes notified to the Commission and respecting a number of requirements, formats and procedures (hereinafter “notified eIDs”). The choice to notify the Commission of all, some or none of the electronic identification schemes used at national level to access, at least, public online services or specific services is up to Member States.

Although the Regulation only imposes obligations for recognition of eID on the public sector, it also foresees that Member States encourage the private sector to voluntarily use eID means in order to extend trust and security to commercial interactions. The Regulation also fosters market development and use of innovative solutions and services, such as mobile signing or cloud signing.

Baseline and points of comparison

Before the Regulation entered into force there was no comprehensive EU cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions for electronic identification, authentication and trust services. The Commission proposal (COM(2012) 238 final) of 4 June 2012 accompanied by the Impact Assessment (SWD(2012) 135 final) identified four general objectives:

- ensuring the development of a digital single market;
- promoting the development of key cross-border public services;
- stimulating and strengthening competition in the single market;
- enhancing user-friendliness (citizens and businesses).

The eIDAS framework was a positive driver for the Member States to build up eID schemes in general. Before eIDAS there was no legal framework to define what are the requirements and features of a national eID system. The European “blueprint” for electronic identification schemes provided by eIDAS gave Member States the reassurance that, if they follow the rules, they would establish robust identity systems underpinning all public transactions and interactions.

While eIDAS plays an undisputed role in the internal market, a lot has changed since its adoption. Adopted in 2014, eIDAS is based on national eID systems following diverse standards and focuses on a relatively small segment of the electronic identification needs of citizens and businesses: secure cross-border access to public services. Since then, digitalisation of all functions of society has increased dramatically. Not least has the COVID-19 pandemic had a very strong impact on the speed of digitalisation. As a result, the provision of both public and private services is increasingly becoming digital. Citizens and businesses’ expectations are to achieve high security and convenience for any online activity. As a consequence, the demand for means to identify and authenticate online, as well as to digitally exchange information related to identity, attributes or qualifications securely and with a high degree of data protection, has increased radically.

Electronic identification

Before the adoption of the Regulation, different types of solutions were introduced on the market, either led by governments to complement paper-based ID cards or provided by the private sector.

⁶ E.g. for eIDs within MSs – they are mapped against outcome based criteria to determine which of the 3 levels of assurance is applicable for both natural and legal persons.

However, no common standards were used and electronic identification of citizens and businesses remained fragmented and in many cases duplicated. In addition, the usage of eID was mostly limited to the access of online services and interactions at national level or for use within a specific sector. An eID issued in one Member State could not be used to access online services in another Member State.

The reasons for this were of both technical and legal nature. Member States used different technological solutions, which led to a **lack of cross-border and cross-sector interoperability**, there was a **lack of a common legal framework to determine the reliability** of the entity issuing the eID, a **lack of legal certainty** on the cross-border use of eIDs and a **lack of rules for liability**, regarding the correctness of the identity.

Before the adoption of the Regulation, there was a **lack of trust and confidence in electronic transactions**, the tools provided, the legal framework and the security of eIDs among the general public. The lack of a common European legal framework hindered security and trust among citizens, businesses and public administrations when interacting online in cross-border scenarios. In addition, there was a lack of awareness of the added value of eID. These factors led to a **limited use of public and private online services**.

As a response to these problems and needs and with the aim to ensure mutual recognition and acceptance of notified eIDs, the Regulation introduced the principle of mutual recognition of eID means to access online public services. By introducing the notification of these eID schemes, the eIDAS Regulation also established a process by which Member States can make their national eID schemes available for **cross-border and cross-sector use**, with the aim to ensure usage of notified eIDs by public and private sector entities.

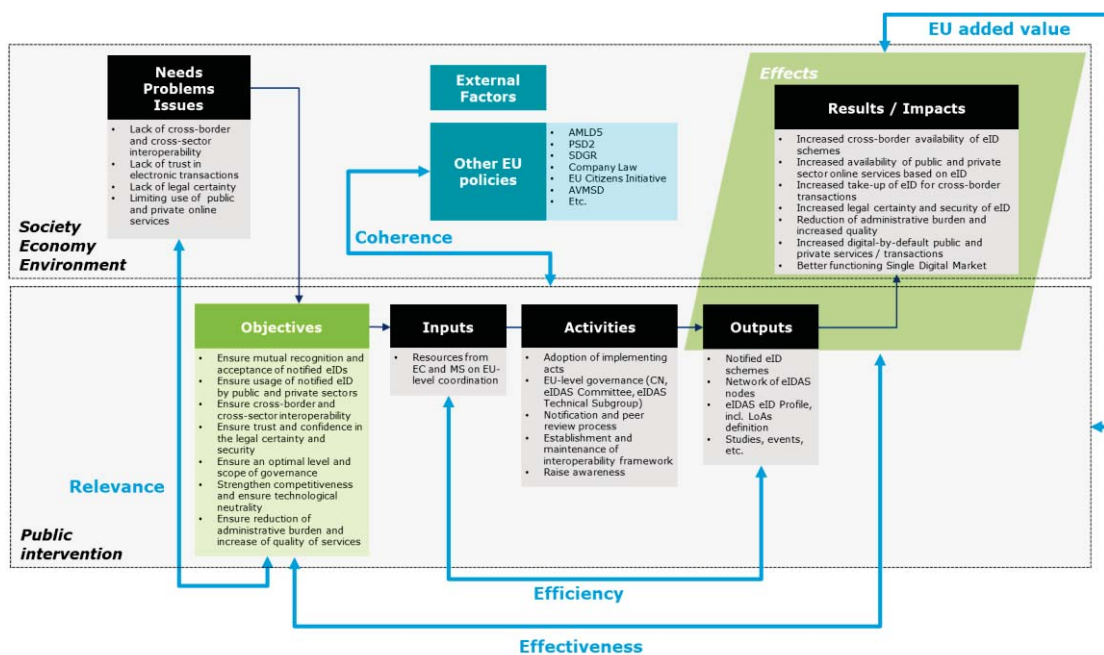
For the use of eID in practice and due to the need for trust, security and data protection, online service providers need certainty that a specific eID gives the appropriate level of assurance for each online service. Hence, online service providers dealing with sensitive information or transactions would require an eID that is highly trustworthy. In order to make this a reality, the eIDAS Regulation introduced assurance framework with minimum technical specifications and procedures defining three levels of assurance – low, substantial and high – for notified eID schemes.

To ensure an optimal scope and level of governance for eID, the eIDAS framework established four bodies involved in the governance of eID - the eIDAS expert group, the eIDAS Committee, the Cooperation Network and the eIDAS eID technical subgroup.

Overall, by setting up a common legal and technical framework for eID, the eIDAS Regulation has tackled important needs and problems in the field of eID, which has the potential to ensure a **reduction of administrative burden and an increased quality of services**. Hereby, the eIDAS Regulation also contributes to the overall objectives of developing a Digital Single Market and promoting the interest and protection of consumers in the EU. Another major factor determining the success in achieving these overall objectives lies within the need and goal to **strengthen competitiveness and ensure technological neutrality** in the field of eID.

The figure below provides a schematic overview of the intervention logic and evaluation criteria, including the needs, problems and issues preceding the Regulation, the objectives it is set to achieve, the activities it initiated, the desired outputs and results and impacts.

Figure 2 - eID - Intervention logic and evaluation criteria



Trust services

The digital transformation of administrative processes and of business relations calls for secure, reliable and seamless electronic interaction and requires increasing the effectiveness of online services offered in the public and private sectors and creating trust in electronic transactions. User confidence in the security of electronic transactions is a condition for their widespread use. European trust service providers play a major role in assuring the security of electronic transactions⁷.

Before the adoption of the eIDAS Regulation, the European regulatory framework in this area covered only electronic signatures (eSignatures) and eSignature creation devices regulated under the **eSignatures Directive**.

A study on the cross-border interoperability of e-signatures⁸ concluded in 2010 that the regulatory framework of the eSignatures Directive remained incomplete and did not sufficiently address challenges, such as market fragmentation, the use of outdated standards⁹ and different implementation, interpretation and levels of supervision by Member States. This led to market distortion for trust service providers which were required to meet different standards depending on their country of establishment and their country of business activity. Divergent implementation and the adoption of varying rules for services at national level also led to the introduction of new categories of signatures in Member States which only differed in terminology creating market confusion.¹⁰

Furthermore, diverging interpretations of the Directive led to cross-border interoperability challenges and to a lack of mutual recognition and acceptance. The eSignature Directive did not lay

⁷ See Chambersign position paper on EU Regulation on eID and Trust Services here: <https://www.dtce.eu/documents/2012/10/dtce-chambersign-position-paper-on-eu-regulation-on-eid-and-etrust-services.pdf>
⁸ Study on Cross-Border Interoperability of e-signatures, see <https://ec.europa.eu/digital-single-market/en/news/crobies-study-cross-border-interoperability-esignatures-2010>
⁹ Standards were not addressed in the eSignature Directive
¹⁰ For example, the ‘universal electronic signature’ was introduced in Bulgaria, the ‘secure electronic signature’ in Lithuania and Poland, or a differentiation was made in France between ‘middle, standard or strengthened electronic signature’.

out common standards for electronic signatures resulting in a patchwork of national legislation.¹¹ None of the Member States implemented the same procedural standards for enforcement, with adverse effects on interoperability and the functioning of the Single Market.

The regulatory challenges impacted the trust service providers in a number of ways. **Service providers** wanting to offer their services in another Member state were faced with **high costs** due to varying technical requirements and the need to comply with the country of destination. The **varying levels of supervision** led to a lack of trust and legal certainty of trust services in the European market, thereby hindering the cross-border uptake of the services. They resulted in an **uneven playing field** with respect to trustworthiness and costs; audit expenses were incurred by the service provider. **Outdated standards** were another issue not addressed in the eSignatures Directive. The Directive did not lay out common standards for electronic signatures resulting in a patchwork of national legislation¹².

The eIDAS Regulation therefore sought to address these issues. An overall objective of the eIDAS Regulation is to establish **trust and confidence in legal certainty and security of trust services** by the introduction of the qualified status. Trust services compliant with the requirements laid out in the Regulation ‘shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form’ i.e. the Regulation provides for non-discrimination of electronic forms vis-à-vis the paper equivalent.

Introducing the concept of qualified trust services is crucial in **ensuring legal certainty, liability and burden of proof**. Furthermore the provisions on security requirements’ provisions aim to ensure an adequate level of security and risk management in the provision of trust services. The Regulation lays down further specific requirements for QTSPs, e.g. by ensuring that when issuing a qualified certificate QTSPs shall verify in trustworthy manner the identity of a person. The QTSP must provide news on any changes to its organisation to the supervisory body, in order for the supervisory body to maintain the trusted list, thereby ensuring **trust and confidence for users**. In order to effectively oversee the provision of trust services, the Regulation aims to ensure an **optimal scope and level of governance**. The Regulation establishes a European wide supervision regime that aims to create a fairer playing field for trust service providers, enhance **trust and confidence in services** offered by a service provider established in another Member State, and thereby **increase the take-up of services** in the European market.

In addition, number of trust services necessary to foster secure and seamless online transactions, were not regulated at EU level:

- Timestamping – validating date and time on an electronic document to prove that the document existed at the given point in time and that it has not been modified since;
- Electronic seal – the electronic equivalent of a seal or stamp applied to a document to guarantee its origin and integrity;
- Electronic delivery – mail registered and delivered digitally;
- Website authentication – certificates that allow verification of a website’s authenticity and its link to a natural or legal person

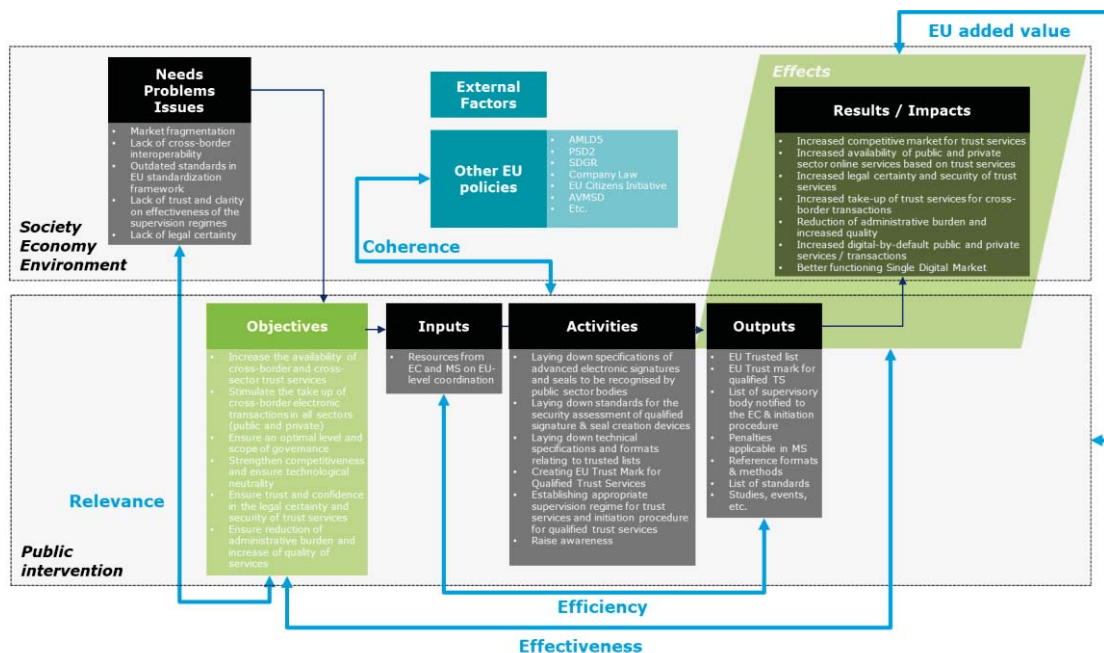
All these measures are aimed at increasing the availability of cross-border and cross-sector trust services and strengthen competitiveness while ensuring technological neutrality. Ultimately this should also lead to a reduction in administrative burden due to increased use of electronic transactions as well as and increased quality of services.

¹¹ Important facts about European Union e-Signature law (2018). See: <https://www.esigngenie.com/blog/european-union-esignature-law-real-facts/>

¹² Important facts about European Union e-Signature law (2018). <https://www.esigngenie.com/blog/european-union-esignature-law-real-facts/>

The figure below provides a schematic overview of the intervention logic and evaluation criteria, including the needs, problems and issues preceding the eIDAS Regulation, the objectives it is set to achieve, the activities it initiated, the desired outputs and results and impacts.

Figure 3 - Trust Services - Intervention logic and evaluation criteria



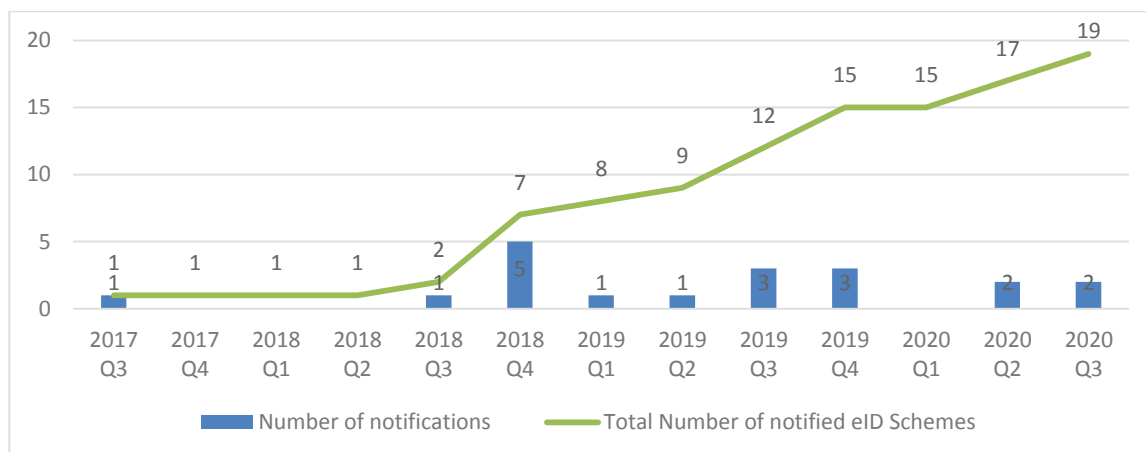
3. IMPLEMENTATION / STATE OF PLAY

Electronic identification

One of the most important implementation indicators of the eID part of the Regulation is the number of the eIDAS **notifications of national eID schemes**. Since the entering into force of this part of the Regulation in September 2017, 14¹³ Member States have notified at least one eID scheme and four¹⁴ Member States have already notified multiple schemes. In total, 19 eID schemes have been notified so far.¹⁵ By April 2021 three Member States¹⁶ have pre-notified their schemes. Since there is no obligation to notify eID schemes under the eIDAS Regulation, several Member States with national eID schemes in place have so far not notified them.

¹³ The United Kingdom notification of UK.GOV Verify (on 2 May 2019) is not included in this analysis.
¹⁴ Belgium, the Netherlands, Italy and Portugal. A number of notified eID schemes includes multiple eID means (e.g. in case of Estonia the eID card and Mobiil-ID, amongst others)
¹⁵ State of Play 8 September 2020: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview>
¹⁶ Sweden, France and Malta

Figure 4 Progress of notifications of eID schemes¹⁷



Although the Regulation states that Member States should not be obliged to notify their national eIDs to the Commission, the expectation and the target set at the institutional level (Strategic Management Plan DG CONNECT 2016-2020) was that by the time the mutual obligation provision enters into force (September 2018), all Member States would have recognised the notified schemes. In the Tallinn Ministerial Declaration on eGovernment of 6 October 2017, Member States agreed to provide citizens and businesses with the option to interact digitally with public administrations, and to ensure timely implementation, and promote the widespread use across sectors, of the eIDAS Regulation, including to undertake the voluntary notification of national eIDs. However, by the end of 2018 seven Member States had done so.

Peer reviews are an essential activity within the notification process. 28 Member States (including UK) and the 3 EEA are eligible to participate in them. So far, 16 countries participated in the 15 peer reviews conducted so far. Following the notification of an eID scheme, Member States have one year to conclude peer reviews and take a position on the eligibility of the scheme for mutual recognition under eIDAS. As of 18 December 2020, European citizens can use national eID schemes from **12 EU Member States** across borders. However, this is only the case provided that the eID means¹⁸ corresponds to the level of assurance “substantial” or “high” and that the eID scheme reaches the minimum level of assurance requested by the service provider. As the use of eID under eIDAS is open to the private sector, businesses can also benefit from this cross-border recognition of eID, however, the conditions for the use of the eIDAS eIDs by the private sector are defined by the Member States and to date these transactions are very limited.

The **eIDAS Network** for eID consists of the eIDAS nodes¹⁹, established at Member State and EU level- including EFTA EEA Countries (Iceland, Liechtenstein, and Norway)-, and interconnects the notified eID schemes connected to the eIDAS node at national level. While most eIDAS nodes are in production, it seems that Cyprus, Ireland, Iceland and Poland are conducting some testing and may therefore not be fully operational. Information for Bulgaria, France, Hungary, Liechtenstein and Romania is missing. Generally, Member States are prioritising the development of their receiving function. The sending function might only be developed once a country has effectively pre-notified an eID scheme. Due to the lack of the monitoring requirements, there is not a complete picture of the use of the eIDAS infrastructure. Some limitations of the implementation showed

¹⁷ This graph is based on the data available on CEF digital and include the notification of UK : <https://ec.europa.eu/cefdigital/wiki/x/iw3oAg>

¹⁸ ‘electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service

¹⁹ The eIDAS Network consists of a number of interconnected eIDAS nodes, which can either request or provide cross-border authentication. It is the responsibility of each country to implement their eIDAS node.

during the evaluation are due to the pending transition period of the notified eIDs, which were not yet subject to the mutual recognition obligation. The success at this point in time would require that all Member States would have fully integrated the technical infrastructure to support the cross-border access to national online public services via notified eIDs and that online private services providers would have found it attractive to rely on notified eIDs.

The Commission has launched several **studies and events** to support the implementation of the eIDAS framework and to cover relevant trends in the field of eID. These studies are partly sector-specific (e.g. banking, higher education, aviation, SMEs, migration), focus on more general principles related to eID under eIDAS (e.g. awareness-raising, user experience) or analyse current trends in eID (e.g. mobile first, biometrics, analytics enabling real-time and continuous authentication, blurring lines between physical and digital worlds, citizen-controlled data, changing identity ecosystem).

Among the **sector-specific** studies, several focus on the potential impact of the eIDAS Regulation on the **banking sector**, as it helps financial institutions to meet legal obligations in the fields of know-your-customer (KYC), Anti-Money Laundering²⁰ and strong authentication of parties²¹. An analysis²² carried out in 2018 on the reuse of eIDAS-based eID in the banking sector concluded that some eIDs created in the banking sector have become available nation-wide while in some other cases banks already participate in a federation of ID providers contributing to a government ID scheme.²³ The study concluded that efficiency gains would best be achieved through a full coverage of the EU with eID notified schemes under eIDAS Regulation and made available for use by the private sector and that the financial sector lacked sufficient understanding of the benefits of the eIDAS Regulation. Although the use of the eIDs under eIDAS is voluntary by the private sector and dependent on the conditions set by the Member States, several eID providers confirmed that the confirmation of the compliance with the eIDAS helped them to gain momentum on the market and facilitated the access to additional services, in particular at the national level.

Another sector in which the use of eIDAS could lead to considerable efficiency gains and reduce administrative burden is **higher education**. A study²⁴ showed in 2018 that identification and student-specific data in the context of the ERASMUS+ programme was manually entered and verified with limits to reliability and considerable administrative burden. With the mutual recognition of eID under eIDAS between Member States, universities are able to exchange identification data of the students in a seamless, reliable and trusted way. However, students still need to manually enter the student-specific data (such as HEI code, student identifier, student email, etc.) and provide the requested supporting documents. Hence, as for the banking sector, an addition of domain-specific attributes to the eIDAS minimum dataset could further **reduce administrative burden**.

In the **aviation sector**²⁵, eIDAS-based eIDs could automatize data entry, reduce error rates and allow for a seamless and smooth customer-journey. At the same time, as in other sectors, the absence of necessary attributes and data (e.g. biometrics) are limiting factors.

In **eHealth**, several Member States have linked national eID solutions to their social security systems. Studies concluded that the current eIDAS framework could allow for the exchange of sector-specific attributes, such as patient ID or the direct notification of an eHealth eID solution²⁶.

²⁰ See 4th Anti-Money Laundering Directive

²¹ See 2nd Payment Services Directive

²² Deloitte (2018): Business proposition of eIDAS-based eID – banking sector

²³ E.g. itsme in Belgium or BankID in the Nordic countries

²⁴ Everis (2018): CEF eID building block for banking and educational domains

²⁵ Deloitte (2018): Business proposition of eIDAS-based eID – aviation sector

²⁶ DIGIT, The use of CEF eID in the CEF eHealth DSI, 2016, see:

The eHealth Network²⁷ (eHN) continues to investigate the reuse of eID for eHealth purposes and some pilots are ongoing.²⁸ The Joint Action²⁹ supporting the eHN by developing strategic guidance and tools in priority areas issued the Common eID Strategy for eHealth³⁰ that can leverage EU regulations and create a holistic approach to eID in eHealth and related ICT services, both for patient and clinician identification, achieving **innovative use of health data** and **interoperability** within and across borders, supported by an increased strength in the security of identification of persons.

Regarding the use of eID under the eIDAS by SMEs³¹, low awareness has been identified as a key barrier for uptake although there is considerable potential for improving user experience, security, liability and operational efficiency of SMEs. As a result, a guidebook, checklist and toolkit for SMEs have been developed³².

Other studies have identified as blocking factors for the uptake of eID, the **lack of awareness** and understanding of the Regulation and its impact³³ and **poor user experience**³⁴, which also discourages private service providers to make their online services accessible via the eIDAS Network for the risk of compromising on the quality of the services they provide.

At the same time, advances in **technology**³⁵ shape the future of eID and may help increase availability and uptake, enhance user experience and mitigate cybersecurity risks³⁶.

Today, not all Member States allow the **use of eID schemes by the private sector operators** established in their own country and abroad (i.e. a national eID scheme cannot be used by the private sector relying party for authentication and identification). As liabilities and costs are not regulated at EU level and incentives differ, the take-up of eID /eIDAS by the private sector is partial and fragmented.³⁷

Trust services

The contribution to the development of an internal market for trust services in the EU is a key result indicators for the implementation of the eIDAS Regulation. Before the eIDAS Regulation, the **service providers wanting to offer their services in another Member State were faced with high costs** due to varying technical requirements and the need to comply with the country of destination rules. European trust service providers could not operate in another Member State without incurring additional costs. These conditions were evidently not favourable for the functioning of the internal market.

https://ec.europa.eu/cefdigital/wiki/download/attachments/37766100/DG%20DIGIT%20-%20The%20use%20of%20eID%20in%20eHealth%20-%20Final%20Report%20v3_0.pdf?version=1&modificationDate=1486488638015&api=v2

²⁷ European Commission, eHealth Network, see: https://ec.europa.eu/health/ehealth/policy/network_en

²⁸ HEALTHeID, eHN update on technical implementation and Member States participation in the HEALTHeID Transfer-athon, November 2019, see:

https://www.spms.min-saude.pt/wp-content/uploads/2020/01/eHN_Nov_2019_HEALTHeID_Final.pdf

²⁹ eHACTION – Joint action supporting the eHealth Network, see <https://http://ehaction.eu/>

³⁰ Common eID Strategy for Health in the EU – Information paper for eHN, October 2020

³¹ Deloitte and The Lisbon Council (2019): EIDAS study on pilots for replication of multipliers

³² <https://ec.europa.eu/digital-single-market/en/eidas-smes>

³³ PwC (2018): Study on a marketing plan to stimulate the take-up of eID and trust service for the Digital Single Market

³⁴ Deloitte (2018): The user experience of eIDAS-based eID

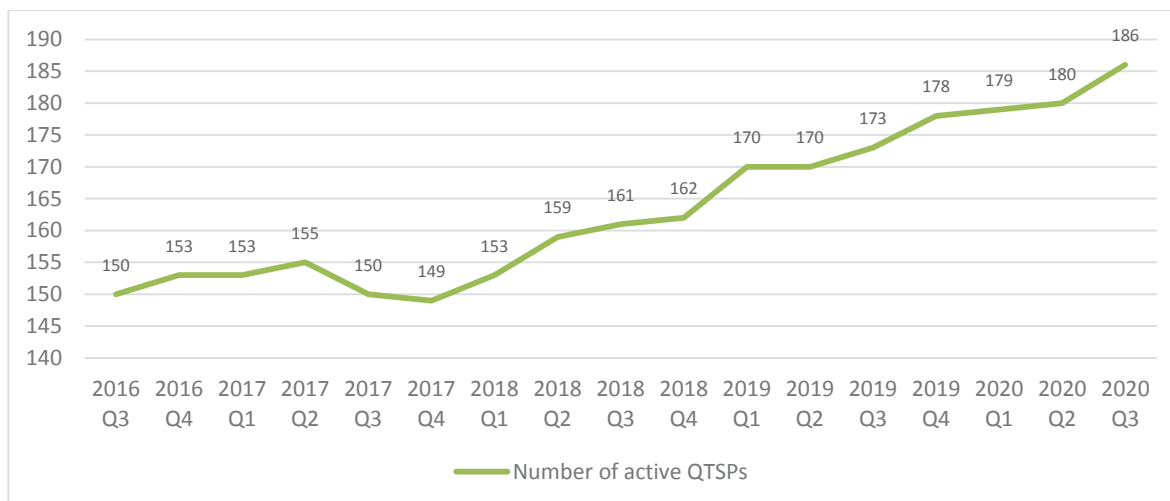
³⁵ These include: mobile solutions, biometrics, artificial intelligence, analytics enabling real-time and continuous authentication, the Internet of Things, citizen-controlled data, analytics and blockchain.

³⁶ Deloitte (2018): Trends in electronic identification – An overview

³⁷ In 2019, the Commission engaged in the discussion between Member States (Cooperation Network) with regard to the terms of access for relying parties other than public sector to the notified eID schemes available via the eIDAS network.

There are currently 202³⁸ active qualified trust service providers operating in 29 of the 30 EU and EEA/EFTA countries. There are further 59 trust service providers without active trust services listed.

Figure 5 Evolution of the number of qualified trust service providers³⁹



Markets with the most active Qualified Trust Service Providers (QTSPs) are Spain (36), Italy (22), France (24) and Germany (12), while Denmark currently does not have any active qualified trust service providers.

Qualified eSignatures are the service provided most on the market, followed by qualified time stamps and qualified eSeals. Out of the five core trust services (Qualified certificate for electronic signature, Qualified certificate for electronic seal, Qualified time stamp, Qualified certificate for website authentication, Qualified electronic registered delivery service), the latter service is the most limited one, featuring only 20 active services in seven Member States at present.⁴⁰

Table 1: Qualified trust services in Europe⁴¹

Type of Qualified Trust Service	Number of active Qualified Trust Services	Number of countries (EU and EEA/EFTA) in which the Qualified Trust Service is active	EU and EEA/EFTA countries in which the Qualified Trust Service is active
Qualified certificate for electronic signature	152	28	AT, BE, BG, HR, CY, CZ, EE, FI, FR, DE, EL, HU, IS, IE, IT, LI, LT, LV, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES
Qualified time stamp	109	23	AT, BE, BG, HR, CZ, EE, FR, DE, EL, HU, IE, IT, LV, LT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified certificate for electronic seal	102	24	AT, BE, BG, HR, CY, CZ, EE, FR, DE, EL, HU, IE, IT, LV, LT, LU, NL, NO, PL, PT,

³⁸ Sourced from the Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 28 April 2021.

³⁹ Abstract from the TL Browser, see: <https://webgate.ec.europa.eu/tl-browser/#/>

⁴⁰ ENISA, 2015, Qualified Website Authentication Certificates

⁴¹ Statistics sourced from Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 8 September 2020

			RO, SK, SI, ES
Qualified certificate for website authentication	51	20	AT, BE, BG, HR, CZ, FI, FR, DE, EL, HU, IT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified electronic registered delivery service	20	7	BE, FR, DE, NL, PL, SI, ES
Qualified validation service for qualified electronic signature	15	10	BE, BG, CZ, FR, LT, PL, SI, SK, ES, SE
Qualified validation service for qualified electronic seal	15	10	BE, BG, CZ, FR, LT, PL, SK, SI, ES, SE
Qualified preservation service for qualified electronic seal	13	9	BG, CZ, FR, HU, MT, PL, RO, SK, ES
Qualified preservation service for qualified electronic signature	12	7	BG, CZ, FR, HU, MT, PL, RO, SK, ES

National supervisory bodies for trust service providers can carry out audits, grant qualified status, and take enforcement action. They also keep the national Trusted List of QTSPs with few exceptions (e.g. AT, DE, PL) and are established in all Member States alongside National Accreditation Bodies.⁴² Conformity Assessment Bodies which are generally private or semi-private, are present in 12 Member States, with numbers differing between seven in IT and one in NL and PT.⁴³

The European List of Trusted Lists (LOTL) comprises all of the trusted lists managed by Member States and information on QTSPs and their QTSs and contains pointers to the locations of publication of the national trusted lists. The European Commission developed a tool that enables its users to browse current trust service providers and trust services – the Trusted List Browser.⁴⁴ Users can browse trust services using various filters, such as the type of service and the country, the name of trust service and signed file.

In order to further ensure the security, legal certainty and the harmonisation of European trust services, standards are developed and maintained for European trust services. The Commission supports the use of ETSI/ CEN standards. The standards for trust services are frequently updated and published in order for trust service market players to ensure that they are following the most recent standards. ETSI standardization in relation to European trust services is currently used for policy requirements⁴⁵, assessment scheme⁴⁶ (conformity assessment) and trust service status lists⁴⁷.

⁴² Compilation of information provided by Member States with regard to the implementation of the Trust Services chapter of the eIDAS Regulation (2019). See here: https://ec.europa.eu/futurium/en/system/files/ged/compilation_ms_information_07052019.pdf Information missing has been compiled by the European Commission for IE, RO and PT, respectively the Irish Department of Communications, Climate Action & Environment, the Authority for Romania's Digitization (ADR) and Portuguese Gabinete Nacional de Segurança (GNS).

⁴³ Compiled list of conformity assessment bodies as defined in point 13 of Article 2 of Regulation (EC) No 765/2008 and accredited as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides against the requirements of eIDAS Regulation (EU) 910/2014, see: https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accruited_cabs-2019-08-23.pdf

⁴⁴ Trusted List Browser. See here: <https://webgate.ec.europa.eu/tl-browser/#/>

⁴⁵ ETSI Standard : ETSI EN 319 4xx series (e.g. EN 319 411-2) and EN 319 5xx series

⁴⁶ ETSI Standard : ETSI 319 403

⁴⁷ ETSI Standard : ETSI TS 119 612

Protocols⁴⁸ for trust service providers providing long-term data preservation services is due to be published soon. Today, there are generally ETSI/ CEN standards for trust services in almost all relevant areas.

4. METHOD

The eIDAS Regulation is substantively split into two parts; electronic identification (chapter II) and trust services (chapter III). Not only is there a difference in the timeline of the entry into force of the legal provisions linked to trust services and eID, but the nature of the frameworks governing eID and trust services fundamentally differ. For the purposes of the evaluation it is key to assess and analyse both domains separately, while also comparing across and looking at the eIDAS Regulation as a whole.

The different implementation period⁴⁹ had some impacts on the evaluation, in particular with respect to the eID part of the Regulation. The majority of the notified eIDs only became subject to the mutual recognition obligation in the course of 2020 or the implementation is yet ongoing. Additional increase in the usage of notified eIDs can be expected in the coming years, as more schemes become available and more citizens become aware of the possibility to reuse their national eIDs abroad.

The present evaluation of the eIDAS Regulation was carried out between September 2019 and December 2020. It builds on evidence collected by an external support study⁵⁰ assessing the performance of the eIDAS Regulation compared with its objectives and whether it remains fit for purpose to deliver the intended results and impacts. The evaluation has been carried out on the basis of data collected from different sources. A more detailed insight is provided in Annex 3. The evaluation draws on data from various sources:

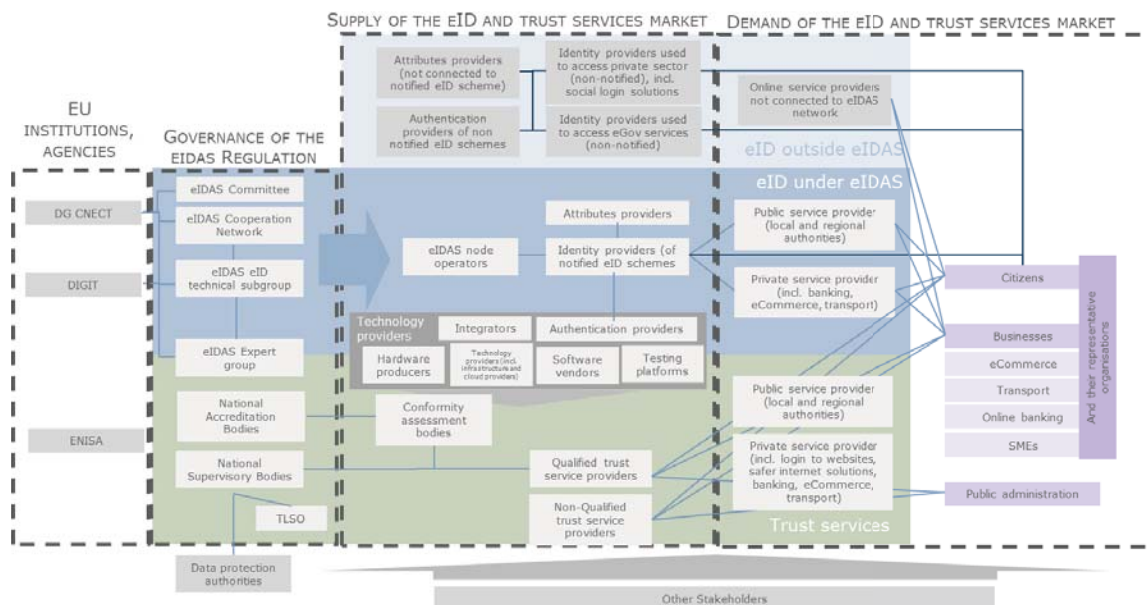
- Open Public Consultation (onwards ‘OPC’ - 24 July to 2 October 2020);
- Targeted Stakeholders consultations including surveys, interviews and workshops;
- External studies;
- Literature review.

⁴⁸ ETSI Standard : ETSI TS 119 512

⁴⁹ The provisions on the trust services entered into force on 1 July 2016 and the mutual recognition obligation of notified eIDs on 29 September 2018.

⁵⁰ Study SMART 2019/0046 evaluating the European Regulation 910/2014 (eIDAS Regulation) has been commissioned by the European Commission Directorate-General for Communications Networks, Content and Technology H4 (DG CNECT H4) and performed by Deloitte , VVA, Spark and ECORYS

Figure 6 Stakeholders mapping



The estimation of the actual number of stakeholders for the categories had to rely on a series of assumptions, which makes the interpretation of the findings more complex. On the one hand, the estimation of the number of active service providers (eID) and non-qualified trust service providers had to rely entirely and exclusively on stakeholder consultation activities, and therefore the findings are of limited reliability. On the other hand, the number of national authorities and eIDAS node operators, eID providers, bodies and qualified trust service providers is continuously adjourning, as the implementation of eIDAS (notification, qualification, set up of nodes) proceeds. Therefore, the aggregate figures refer to a hypothetical year, where all stakeholders begin operations, sustain initial costs, sustain recurring (yearly) costs once, and enjoy (yearly) benefits once.

The data gathering activities, in particular with respect to the implementation of the eID part of the Regulation, has been carried out at different levels – workshops, surveys and the scoping interviews with the Member States representatives, the service providers, the experts, follow up interviews after submitting the inputs to the online surveys and the literature analysis. Certain limitations in the data gathering are due to the lack of monitoring and reporting obligations in the Regulation, which limits the access to reliable data, in particular for the implementation of the eID part of the Regulation, which relied during the evaluation on the openness and willingness of some of the Member States to share the data on the usage of the national eIDAS infrastructure for cross border transactions.

Regulatory efficiency was assessed through a **Cost-Benefit Analysis (CBA)** to quantify and monetise the main costs and benefits, thereby providing a baseline scenario for future assessment and possible policy intervention. The collection of quantitative data proved to be a difficult task for the consulted stakeholders. The most critical aspect was the distinction between duties (and thus costs) that were directly linked to the eIDAS Regulation and the other obligations that stakeholders incurred due to related initiatives (e.g. the provision of the eID service at national level). A large part of the sample of stakeholders, however, was reluctant in giving quantitative values or simply did not have in place a monitoring system able to gather relevant data for the CBA.

The CBA has been particularly challenging due to the fact that in most cases the stakeholders that are targeted by the Regulation are at the same providing electronic identification services at national level. This means that respondents to survey and interviews found it particularly challenging to disentangle the costs only due to the Regulation from the other costs incurred due to

the provision of these services (either eID or trust services) at national level due to other regulatory sources.

The calculations provided in the report rely on estimates reported by stakeholders and should be considered as indicative averages by category of respondent. For all types of organisations either providing the eID or the trust services, costs and benefits may change considerably due to several variables: size of the country, number of operators, technological take-up of eIDs and trust services, size of the organisation and market position.

Given these limitations, the final estimates are based only on a sub-sample of responses.

A series of **strategic interviews** with individuals and organisations provided strategic input to better define data collection strategies and questionnaires.

Targeted stakeholder surveys and interviews allowed to collect views, primary data and evidence for the analysis of key evaluation questions identified through desk research and strategic interviews.

In the **Open Public Consultation**, 318 respondents expressed their views on the evaluation questions and in particular on drivers and barriers to the development and uptake of eID and trust services.

To gather primary data a number **surveys** targeting key stakeholders were carried out:

- **Member State representatives** – The objective of this survey was to gather the views of Member States’ representatives in the eIDAS Cooperation Network, eIDAS Expert Group and operators of eIDAS nodes on the functioning of the Regulation, the interaction of the Regulation with other initiatives and on the costs associated with its implementation.
- **Service providers (Relying parties)** – The objective of this survey was to gather the views of both public and private service providers on the functioning of the Regulation and its impact on the services they provide.
- **Supervisory Bodies, Conformity Assessment Bodies, Accreditation Bodies** – The objective of this survey was to gather the views of the different Bodies responsible for the supervision of trust services with specific regard to governance and associated costs.
- **Trust services providers and representative organisations of trust service providers** – The objective of this survey was to gather the views of both qualified and non-qualified trust service providers on the functioning of the Regulation and its market impacts.
- **Identity providers and representation organisations of identity providers** – The survey gathered the views of both notified and non-notified identity providers on the functioning of the Regulation and on its market impacts.
- **Technology providers**, providers of trust services not covered by eIDAS, representative organisations of technology providers and standardisation bodies – This survey gathered the views of relevant experts not targeted in other surveys in order to gather a complete view on the functioning and impact of the Regulation.

5. ANALYSIS AND ANSWERS TO THE EVALUATION QUESTIONS

5.1 Effectiveness

The evaluation of the effectiveness of the eIDAS Regulation is based on the general, specific and operational objectives of the Regulation (as described in Section 2). Introduction of a common legal and technical framework for eID aimed at tackling important needs and problems in the field of eID, which had the potential to **ensure a reduction of administrative burden and an increased quality of services**. The eIDAS Regulation also aimed at contributing to the overall objectives of developing a Digital Single Market and promoting the interest and protection of consumers in the EU. Another major factor determining the success in achieving these overall

objectives lies within the need and goal to **strengthen competitiveness and ensure technological neutrality** in the field of eID.

Overall in the field of trust services, the eIDAS measures aimed at **increasing the availability of cross-border and cross-sector trust services** and **strengthen competitiveness** while **ensuring technological neutrality**. Ultimately this should also lead to a **reduction in administrative burden** due to increased use of electronic transactions as well as and **increased quality of services**.

The intervention logic, including a schematic overview of the needs, problems and issues preceding the eIDAS Regulation, the objectives of the intervention, the desired outputs and results and impacts are further detailed in Annex 3.

This section follows a bottom-up approach, analysing first the operational objectives, most of which are sub-categories of the specific objectives, which then feed into the general objectives.

Q1. To what extent has the Regulation met its operational objectives?

Electronic identification

Mutual recognition and acceptance of notified eIDs

One of the main goals of the eIDAS Regulation is to ensure mutual recognition and acceptance of notified eID schemes. The obligation of mutual recognition consists in ensuring that if electronic identification is required under national law or by administrative practice to access an online public service provided in one Member State, eID schemes notified under eIDAS and issued by other Member States shall be recognized, as long as they can provide the minimum level of assurance required by the specific online public service. Member States have up to one year to adapt their respective technical systems between the publication of the notification of an eID scheme in the Official Journal of the European Union⁵¹ and the obligation of mutual recognition of this eID scheme by other Member States.

The acceptance of notified eID scheme relies therefore on two conditions:

- the national eIDAS node of the receiving country needs to be operational (“in production”); and
- the service provider in the receiving country needs to be connected to the national eIDAS node to offer the possibility to use notified eID schemes to access the respective services.

To date 14 Member States have notified in total 19 eID schemes.⁵² The notification is voluntary for the Member States and the eIDAS allows for the notification of the eID schemes endorsed by the Member States. The evaluation showed that the required endorsement is seen as a barrier for the private sector eID providers. To make use of cross-border authentication through eIDAS more attractive for end users, the user experience needs to be improved overall. Many Member States, citizens, businesses and other stakeholders have agreed in the OPC and targeted surveys that an important factor is enabling mobile technologies, however, there is a need to remain technologically neutral.

How eID schemes and systems have been evolving in Member States is also subject to cultural, organisational, and other differences. The design of the notification model in the Regulation reflects these differences by requiring that notified national eIDs can be owned either by the Member States, developed under their mandate, or provided independently but endorsed by the Member State. For a Member States it is more straightforward to notify and take liability of eID schemes they control. When Member States have functioning eID schemes provided by the private

⁵¹ [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020XC0821\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020XC0821(01)&from=EN)

⁵² See Figure 4 for further details of notifications

sector (e.g. banks or telecom companies), they might hesitate in notifying those schemes since it would imply accepting the liability for the functioning of a scheme they do not control, in the cross-border context. In cases where Member States have no control on the provision of a private sector scheme, they may be reluctant to take such liability without firstly clarifying the liabilities and responsibilities in the national regulatory framework that governs the notified eID provided by the private sector provider.

The reasons for not notifying national eIDs by a number of Member States vary and rely on a combination of country-specific internal factors, of disincentives stemming directly from the regulatory regime under eIDAS or from lack of demand for cross border authentications to online public services. An important reason for not notifying an eID scheme is firstly that certain Member States have not used eID schemes widely at national level. Notification would require developing such a scheme, thus implying the deployment of substantial expertise and resources. The development of an eID scheme is thus assessed against other national priorities.

Status of national eIDAS nodes

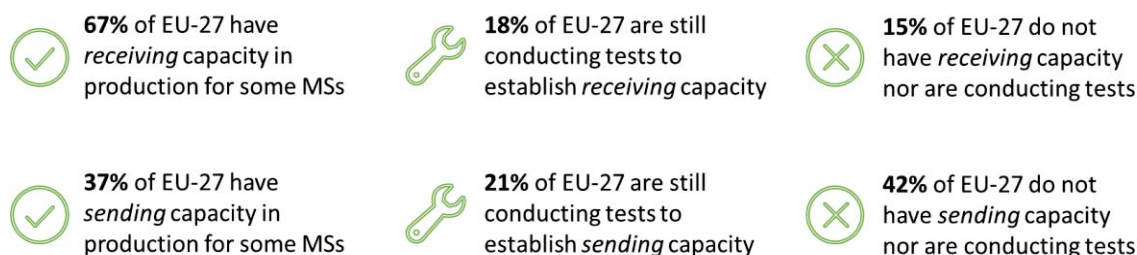
As the eIDAS Regulation does not harmonise the technical standards of national eID schemes for the purpose of their interconnection, technical nodes (“eIDAS nodes”) are necessary to ensure the interoperability of the different national eID schemes notified under eIDAS. In order to support outgoing and incoming identification requests, an eIDAS node is composed of two functions: receiving and sending. The receiving capacity enables the Member States to accept authentications originating from other Member States. The sending capacity is necessary to enable citizens to authenticate for services in another Member State. One incentivising factor for the deployment of the interoperability framework was EU funding for eIDAS nodes, which in turn also helped to improve authentication security in some Member States where it was implemented centrally.

State of Play Receiving Capacity: In September 2020, only 22 out of 30 countries⁵³ had enabled the receiving function of their eIDAS nodes. Four other eIDAS nodes are still testing their receiving capability, while five eIDAS nodes are not operational.

State of Play Sending Capacity: In September 2020, 19 eID schemes of 14 Member States had been successfully notified, however not all of these 14 Member States had nodes with sending functions fully operational.⁵⁴

In addition, not all nodes in production are connected to all the nodes of Member States that have notified an eID scheme. Connections are created and tested manually and are not automated at EU level.

Figure 7 eIDAS node sending and receiving capacity across EU⁵⁵



⁵³ 27 EU Member States plus Iceland, Norway, Liechtenstein.

⁵⁴ N.B. For some of the notified schemes the 12 months period for the implementation (following the date of publication of the eID scheme in OJEU) has not yet elapsed.

⁵⁵ Source: European Commission, cross-border interoperability testing, collaborative platform of EU-27 experts (not accessible to the public)

Overall, the operational state of eIDAS nodes is not satisfactory and several Member States appear in non-compliance with the Regulation. The lack of reporting and monitoring mechanisms for the eID framework in the Regulation limits the effectiveness of the enforcement. Most of the non-compliance issues are related to the implementation of the interoperability framework that have been identified in the course of the evaluation process and testing surveys. Some of the identified non-compliance findings are being gradually solved at national level as increasingly notified eID schemes are becoming subject to mutual recognition obligation.

Status of service providers' connection to the eIDAS network and availability of services








eIDAS nodes in production for both the sending and receiving Member State is a first condition for a successful cross-border authentication. The second condition is the connection of service providers to their national eIDAS node and the third condition is an actual offer for citizens and businesses from abroad to authenticate with their notified eID on their website or application.

There is currently no monitoring and no repository for the number of service providers connected to national eIDAS nodes. Estimates by Member State range from less than 50 to more than 5000, but cannot be verified. In addition, the fact that a service provider is connected does not mean that a cross-border authentication will be possible and successful. Consequently, this indicator cannot be used to evaluate the effective access of citizens to cross-border public services.

The number of services available and the effective possibility for citizens to access them highly depends on the architectural choices of the Member States with regard to their national identity systems. Member States that have centralised their eGovernment services on a central platform or who have put into place a national identity gateway are more likely to enable a good access to the eIDAS network and to effectively recognise notified eID schemes as a valid authentication means on their platforms. In such cases, a “national module” is integrated on service providers websites. The connection of the national authentication gateway to the national eIDAS node means that from one day to the other, all connected service providers that had already adopted the module can now consume identities received via the national eIDAS node. Member States that do not have such gateways or centralised eGovernment platforms need to enable bilateral connections to their national node for every single service provider.

To review the level of acceptance of notified eIDs, the Commission has assessed the possibility to authenticate for seven key public services for cross-border users. The list of key services was determined based on feedback received from Member States that had performed user research and/or analysed statistics of cross-border usage.

Figure 8 Key public services for authentication with eID in Europe

-  Declare Tax
-  Criminal Record Check
-  Apply for or Convert Driving License
-  Apply for pension
-  Obtain residence certificate
-  Access Social Security Services
-  Apply for University

The review shows that across all EU Member States, only 14% of providers of these 7 key services allowed cross-border authentication with eIDAS/eID, while 44% of providers allowed for sign-in only via a national eID.⁵⁶ In conclusion, the large majority of providers of seven key public

⁵⁶ Source: European Commission, Data collection performed by the CEF eID Building Block

services do not offer eIDAS authentication to cross-border users. This suggests the conclusion that the eIDAS framework has not been able to effectively implement mutual recognition of eID and cross-border access to public services and European citizens are faced with multiple obstacles to use their notified eID schemes across borders.

Cross-border interoperability of eID

The eIDAS framework requires that notified national eID schemes shall be interoperable and an interoperability framework is established for this purpose.⁵⁷ An implementing act defines the architecture of the eIDAS network based on national nodes and it foresees the adoption of technical specifications notably for the eIDAS minimum data set and message format, as well as links to the assurance levels of the notified eID schemes.

As part of the Open Public Consultation, only 24% of respondents agreed that the eIDAS interoperability framework sufficiently supported the mutual recognition of the eID schemes while 43% disagreed.

The interoperability of the eIDAS network can be assessed in several dimensions:

- **Technical interoperability** has been ensured through the creation of a network of nodes based on common technical specifications. The Commission provides technical assistance to Member States⁵⁸ and ready-made solutions to facilitate the set-up and maintenance of their nodes which is used by more than half of Member States.
- **Organisational interoperability:** Member States have raised issues linked to the matching of eIDAS/eID identities with an existing national profile. There is currently no process at EU level to avoid that one person owns multiple eIDs issued under different notified eID schemes. This can lead to denial of access in some cases where the receiving Member State cannot exclude duplication. In addition, non-harmonisation of the minimum data set which is communicated in an authentication can also lead to denials of service. Some service providers require a national registry number to grant access to online public services, however not all Member states issue such a number. Consequently cross-border users may be automatically denied access if the eIDAS authentication does not include such number. Obtaining a national registry number often requires physical presence. This is an obstacle for users from abroad even in case they are eligible to obtain a national registry number and to access a service.⁵⁹
- **Semantic interoperability** is enabled by the eIDAS attributes profile (technical specifications). These specifications are continuously updated by the eIDAS eID technical subgroup and no major difficulties have been reported.

The usage of notified eID by public and private sectors

The decentralised nature of the eIDAS network makes it difficult to obtain specific data on the usage of notified eID schemes by public and private sectors. Few Member States have put in place modules allowing to keep track of the statistics of usage of their eIDAS nodes. To assess the usage of notified eID schemes, a number of criteria at the supply and demand side are relevant:

- A critical mass of eID schemes must be notified;
- Relying parties must be connected to the national nodes;

⁵⁷ COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) 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 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0001

⁵⁸ Technical assistance is provided through the Connecting Europe Facility (CEF), eID Building Block.

⁵⁹ Some Member States, including the Netherlands, Belgium, Luxembourg and Latvia, have introduced at least partial remedies.

- Private service providers must be entitled to access the domestic node, foreign nodes and notified identity providers;
- Citizens and businesses must have a need to access a service across borders and must be aware about the possibilities to use their national eID for this purpose;

In theory, 59% of the EU population currently has access to a notified eID scheme. A limited number of Member States have provided the number of relying parties connected to their eIDAS node and the situation can vary considerably between Member States depending on size and organisation of their public services: in some countries, each municipality provides some specific services and would therefore need to connect to the national node while in other countries, key public services are provided centrally.

However, the number of services connected to the national nodes is considerably smaller than the number of services declared as being accessible via the domestic eID scheme. On the basis of available data it seems that only about half of the services accessible through domestic eID are connected to the national eIDAS node.

Table 2: Number of relying parties connected to the national eID scheme

Member State		2017	2018	2019	2020	Comments
Belgium (FAS)⁶⁰			1000			Public services only
Czech Republic (eID card)⁶¹					79	
Germany (eID card)⁶²					95	
Netherlands (DigID)⁶³				663	(Target: 12 000)	
Netherlands (eHerkenning)⁶⁴		260	330	393		
Italy (SPID)⁶⁵	Public				4 478 (Target: 10 000)	Data from 30/07/2020
	Private				11	Data from 03/06/2020
Portugal⁶⁶			150		202	Public and private
Luxembourg⁶⁷	Public		>200			
	Private		6			

The number of cross-border authentications and especially the number of receiving transactions provides an estimate on the usage of notified eID schemes, as it is related to the number of use cases where citizens request access to an online service across borders.

⁶⁰ Source: unpublished Member State data

⁶¹ <https://www.eidentita.cz/Home/Ovm>

⁶² https://www.personalausweisportal.de/DE/Service/Downloads/Erteilte_Berechtigungszertifikate/Erteilte_Berechtigungszertifikate_node.htm

⁶³ Source: unpublished Member State data

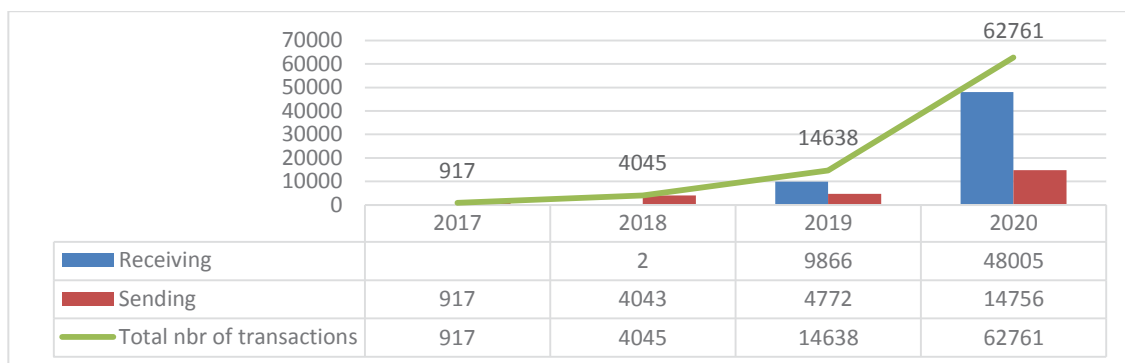
⁶⁴ Source: unpublished Member State data

⁶⁵ <https://avanzamentodigitale.italia.it/it/progetto/spid>

⁶⁶ <https://dados.gov.pt/pt/datasets/autenticacoes-realizadas-por-entidade-e-por-certificado/#>

⁶⁷ Source: unpublished Member State data

Figure 9 Evolution of the number of yearly cross-border authentications⁶⁸

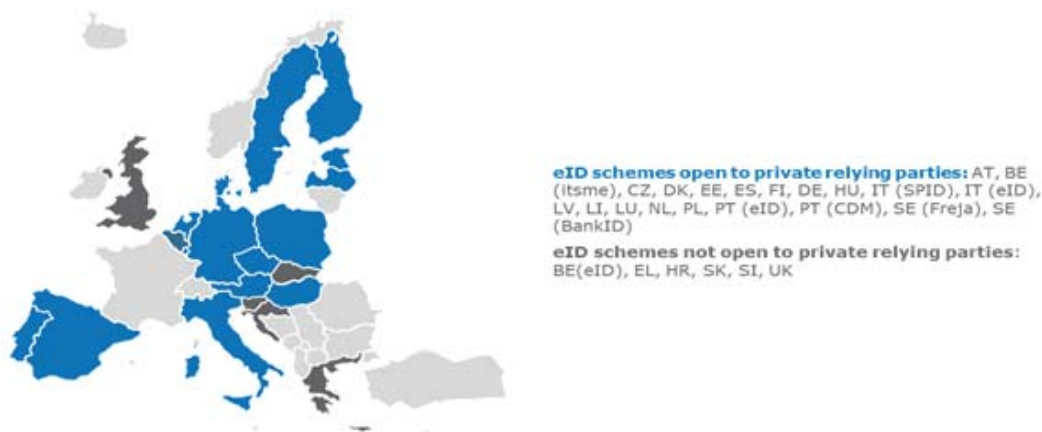


The evolution of the number of transactions in certain Member States⁶⁹ confirms that the usage of notified eID schemes is increasing progressively since September 2018, as more and more eID schemes become available for cross-border use.

The acceptance of notified eIDs is only mandatory for public sector service providers. The usage of notified eIDs by the private sector is limited by two reasons:

- each Member State remains free to set the conditions for the reuse of its national eIDAS infrastructure by the private sector and for the sharing of the minimum data set of its national eID scheme with private service providers;
- private service providers are not subject to a mutual recognition obligation and can recognize notified eID schemes on a voluntary basis.

Figure 10 - eID schemes open to private relying parties⁷⁰



17 Member States have at least one national eID scheme in place that accepts private service providers but only 12 Member States have notified such eID scheme. This limits cross-border availability for private service providers and makes it difficult to build a business case given the difficulties for private service providers to identify available eID schemes and actual market size that they will be able to reach. For example, in the Czech Republic,⁷¹ holders of the national eID

⁶⁸ Cumulative cross-border authentication for a selection of countries: Austria, Czechia, Estonia, Netherlands, Luxembourg, and Sweden

⁶⁹ Based on data provided by the Netherlands.

⁷⁰ Data collected for the Cooperation Network in September 2019. The Belgium itsme® eID is available at the national level to private relying parties. However, only the usage of itsme® via FAS (Federal Authentication Service) to access online public services has been notified.

⁷¹ Identita.cz, Qualified online service providers, see : <https://www.eidentita.cz/Home/Ovm>

can use it to access health insurance companies⁷², online gaming and betting websites⁷³, and a law firm⁷⁴ on top of eGovernment services. The Danish NemID can be used to authenticate to online banking.⁷⁵ In Germany, the list of authorised relying parties is also published and includes banks, notaries, pension insurances and system providers for accountants and attorneys.⁷⁶

To assess the potential cross-border usage for public services, different proxies can be used. According to Eurostat, in 2019 less than 4% of EU citizens of working age were residents of another EU Member State than where they hold their citizenship⁷⁷. In principle, they should be able to use one eID to access public services in both Member States. In addition, there are online public services where user authentication is needed and that can be used by e.g. tourists (about 30% of EU population travel yearly to another Member State) such as buying tickets for public transport, museums or subscribing to bike rentals.

A possibility for assessing the overall potential of eID use is relying on existing use as proxies. Available data from some Member States (e.g. NO, SE, EE, LV, LT), where user authentication solutions are widely re-used by different service providers, authenticating oneself with a legal identity is done roughly around 20 times per month, of which 1 is in the public sector. If that relationship is extrapolated to the EU level, the potential for the EU could be assumed to be roughly 100 billion user authentications per year of which 5 billion in the public sector. On the basis of these assumptions, for example, if expected 3-4% of EU population living in another Member State only use eIDAS in the current scope, the potential of eIDAS authentications in this case would be 150 million authentications per year.

Ensure maximum reduction of administrative burden and increase of quality of services

The targeted stakeholder consultation indicated that the eIDAS Regulation has reduced administrative burden and increased quality of services for eID. In the OPC, a majority of respondents refer to time savings (77% of respondents), to a simplification of administrative procedures (74% of respondents), to cost savings (68% of respondents) and an increase in service quality (65% of respondents).

Reduction of administrative burden is related to the eIDAS Regulation itself and to other related EU legislations which build on the eIDAS ecosystem, such as the Single Digital Gateway Regulation (SDGR). The SDG Regulation enables users to authenticate remotely using their eIDAS notified eID to initiate an exchange of evidence to perform administrative procedures across borders following the ‘once-only’ principle.

For public services, eID eases the administrative burden of operational transactions. But there are also benefits for business. Estonia reports that thanks to eID and the digitalization of its administrative procedures, it is possible to establish a company in Estonia in just under 3 hours, including from abroad.⁷⁸

However, the eIDAS Regulation has not achieved its full potential regarding its contribution to a reduction of the administrative burden, as some obstacles such as physical presence to obtain a

⁷² <https://www.ozp.cz/> and <https://portal.cpzp.cz/>

⁷³ <https://www.sazka.cz/>

⁷⁴ <https://www.ak-vych.cz>

⁷⁵ <https://www.netbank.nordea.dk/netbank/index.jsp>
<https://danskebank.dk/privat/find-hjaelp/netbank-letbank-og-apps>

⁷⁶ Bundesministerium des Innern, für Bau und Heimat, Granted authorization certificates, see: https://www.personalausweisportal.de/DE/Service/Downloads/Erteilte_Berechtigungszerifikate/Erteilte_Berechtigungszerifikate_node.html

⁷⁷ Eurostat, EU citizens living in another Member State - statistical overview, see: https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

⁷⁸ <https://e-estonia.com/solutions/e-identity/mobile-id/>

national registry number and official registration in another Member State persist. For instance, requesting a grant for university studies requires to be officially registered with the local authority. This often requires acquiring a local eID solution.

Ensure trust and confidence in the legal certainty and security of eID

Vulnerabilities may impact the trust and confidence in the security of eID⁷⁹. However, stakeholders consulted as part of the evaluation indicate that the eIDAS Regulation has ensured trust and confidence in the legal certainty and security of eID increasing certainty on the users' identity (73% of respondents), service security (66% of respondents) and clarity on the liability of the provider of the electronic identity (51% of respondents).

Both Member States and industry actors have raised some concerns that current tools for **eID security breaches** are not effective and that eID incident management is not adequately regulated at the EU level. In case of reasonable doubts or proof that a notified eID scheme is victim of a security breach, relying Member States do not have the possibility to suspend its usage.

The different forums established by the Regulation on the cooperation between the Member States (e.g. the Cooperation Network or eID technical subgroup) are working with ENISA on an incident management tool. A pilot has been initiated with ENISA to adapt current reporting tools to the specific case of eID under eIDAS but to date no general solution has been rolled-out towards Member States. Communication channels were established between Member States following the discovery of a vulnerability in the CEF eID sample software of the eIDAS node in summer 2019.

Some stakeholders question the **need of maintaining the level of assurance (LoA) "Low"** in the eIDAS Regulation in future as it was barely used and would not provide the necessary guarantees for the eID to be trusted.

Finally, **liability rules are not harmonised** across Member States, which creates legal insecurity for service providers. Liability rules are set by the notifying Member State and maximum amounts differ considerably.

Trust services

Ensure trust and confidence in the legal certainty and security of trust services

In the view of the respondents of the Open Public Consultation, the eIDAS Regulation has successfully contributed to ensuring legal certainty on the liability and burden of proof with respect to the provision and use of trust services⁸⁰. Furthermore, the eIDAS Regulation is seen to have successfully defined the legal effects of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and electronic documents.⁸¹

Trust and confidence in the security of trust services has also been ensured by regulating the supervision and security requirements for trust services including the requirements imposed on qualified trust service providers on the EU trusted list. Trust service providers and supervisory authorities agree to a large majority that the procedure to follow in case of security breaches is adequate and trust service providers also confirmed to more than 70% that the Regulation had overall ensured trust and confidence in the security of trust services.

A number of specific issues linked to the lack of a harmonisation on some aspects were raised by stakeholders:

⁷⁹ Recent examples:

<https://sec-consult.com/en/blog/2019/10/vulnerability-in-eu-cross-border-authentication-software-eidas-node/>

<https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf>

⁸⁰ 84% of respondents agreed that the use of trust services under the eIDAS Regulation has ensured legal certainty.

⁸¹ Consulted trust service providers confirmed at more than 60% that the burden of proof in relation to the liability for qualified and non-qualified trust services providers is adequate, as well as the legal recognition.

- **Legal certainty of remote signatures:** An amendment to Commission Implementing Decision 2016/650 should reference standards CEN EN 419 241-2 and CEN EN 419 221-5.
- **Link between eSignature to an eTimestamp:** The eIDAS Regulation does not regulate a securely link with the result that the time of signing cannot be relied upon by third parties.
- **Common approach with regard to vulnerabilities and incidents reporting:** The FESA and ENISA Article 19 Expert Groups suggest adoption of an implementing act defining the technical and organisational measures to manage risk.
- **Update of Qualified Electronic Signature Creation Devices (QSCDs):** QSCDs are certified with no time limit although vulnerabilities and new requirements are identified. Some stakeholders recommend to increase the periodic assessment of vulnerability and to set a validity limit for such devices.
- **Termination of Qualified Trust Services:** FESA observes that the lack of requirements on the termination of Qualified Trust Services leads to different practices between Member States.
- **Verification of Identity:** Trust service providers issuing a qualified certificate must verify in accordance with national law, the identity and if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued. Currently article 24 of the eIDAS Regulation requires identity verification by physical presence or by using "other identification methods recognised at national level". The non-harmonisation of these practices raises challenges regarding the trust into the security of services and a common level playing field.
- **Transparency of audit results:** Some stakeholders call for more transparency on audits results to increase trust between Member States, international actors and to remedy the lack of harmonisation of some governance aspects.

Reduce administrative burden and increase the quality of service

A majority of respondents to the OPC agreed that the eIDAS Regulation has led to time savings (85% of respondents), simplification of administrative procedures (77% of respondents), cost savings (72% of respondents), an increase of service quality (69% of respondents) and enhancing user friendliness (61% of respondents).

Limiting factors mentioned by stakeholders include a lack of awareness (50% of respondents), a lack of availability for relevant services (39% of respondents) and a lack of user-friendliness and accessibility for persons with disabilities (36% of respondents). A further 10% of respondents considered trust service solutions too expensive.

Among the consulted trust service providers, 75% considered that the eIDAS Regulation had a **positive impact on the quality of trust services** offered on the EU market and on user satisfaction.

Ensure cross-border and cross-sector interoperability of trust services

A majority of respondents of the stakeholder consultation agreed that interoperability has been ensured with respect to eSignatures (57%), eSeals (52%) and eTimestamps (59%) while 26% of respondents considered that the eIDAS Regulation had failed to ensure the interoperability of trust services. Concerning Qualified Website Authentication certificates (QWACs), a majority of stakeholders (66% of respondents) considered them as not sufficiently interoperable.

Consulted trust services providers expressed some reservations with regards to the link between the introduction of the eIDAS Regulation and the increase interoperability of trust services in Europe. 30% of respondents did not believe that the legal framework led to an increase in interoperability. Some stakeholders considered that most of the trust services' interoperability is linked to an ongoing work of standardisation organisations that would have performed this work with or without the eIDAS Regulation. Moreover, some national dispositions define specific requirements

for trust services' certificates, forcing operators to use different types of certificates in different Member States, effectively reducing their interoperability.

Electronic documents

Chapter IV of the eIDAS Regulation defines the principle of non-discrimination of the legal effects of electronic documents and their admissibility in legal proceedings. As part of the OPC, 70% of respondents agreed that the legal effect provided to electronic documents by the eIDAS Regulation helped increase their take-up and admissibility in legal proceedings.

The European Blockchain Services Infrastructure (EBSI) considers that the current definition of electronic document under eIDAS (any content stored in an electronic form, in particular text or sound, visual or audiovisual recording) would mean that blocks in a blockchain in view of Self Sovereign Identity concepts would equally benefit from the legal effect granted to electronic documents under eIDAS.⁸²

Q2. To what extent has the Regulation met its specific objectives?

Electronic identification

Increase availability and take-up of cross-border eID schemes

One of the key performance indicators of the eIDAS framework is the number of notifications of eID schemes. To date, 19 Member States have notified at least one national eID solution.⁸³ Following the notification of an eID scheme, Member States have 12 months to ensure acceptance for authentication to national public online services. As of 13 September 2020, citizens of 11 Member States can use eID notified under eIDAS across borders and Member States are obliged to recognise them for access to their online public services provided they match the minimum level of assurance requested by the service provider (at least “substantial” or “high”).

The number of notifications has been steadily progressing with several countries reporting their intention to pre-notify eID schemes. However, some Member States have raised concerns with the difficulty they may face to notify private sector schemes used at the national level to access eGovernment services due to the absence of a commercial model at the EU level and possibility for private identity providers to recover their costs.

While the availability of notified eID schemes is progressing, the actual take-up/ usage in terms of the number of cross-border authentications performed has been limited.

The limited data of cross-border authentications provided by Member States shows that numbers remain low (<10 000 authentications per year) compared to the usage of eID at domestic level (> millions authentication per year). However, there is a clear trend towards an exponential growth of such transactions in the last years for those Member States where data has been provided (cf. Figure 9).

Regarding domestic use of eID data availability is better. Sweden clearly stands out in this table in terms of the total number of transactions and transaction per inhabitant. This is due to the fact that the Swedish eID is provided by the banking sector and used in private sector transactions mainly, while less than 7% of the total 4.1 billion requests performed in 2019 are related to public sector services which makes it comparable to the number of public sector transactions in Denmark and the Netherlands in that same year.

The number of unique users per eID scheme is not a sufficient indicator for the take-up of eID as it does not indicate active use. This is particularly relevant in countries that issue eID means (such as

⁸² Dr. Ignacio Alamillo Domingo, SSI eIDAS Legal Report, see:

<https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report>

⁸³ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview>

national electronic ID cards) to the entire population⁸⁴. Other eID means are taken up voluntarily. Coverage varies between 1% to 96% or even 102% as in the case of Estonia⁸⁵, but this data cannot be directly compared. In general, the availability and uptake of cross border eID schemes is progressing. The growth at domestic level in the usage of national eID schemes will positively impact the further use of notified eID schemes at the European level.

Stakeholders agree that the eIDAS framework has fostered the topic of eID high on the agenda of the different EU Member States. Compliance requirements with the eIDAS Regulation have pushed Member States to integrate eID in their respective eGovernment strategies and recognized it as a key enabler for the digital transformation of the European public administration and digital single market. However, the effective uptake and use of notified eID schemes for cross-border transactions remains low.

Ensure a governance framework providing sufficient legal certainty, trust and security of electronic transactions throughout the EU

The eIDAS Regulation has established a governance framework for the eID chapter of the Regulation. The key forum of decision and coordination is the Cooperation Network. Overall, members of the Cooperation Network consulted consider that the current governance is effective and adequate.

However, there are concerns of Member States regarding the effectiveness and efficiency of the current system of notification and peer review established to support mutual recognition between Member States. Member States criticise the **overall length of the procedure to notify an eID scheme** which has taken in the past 9 months in average from pre-notification to publication in the official journal. Given that there is a 12-month delay for the application of mutual recognition following the publication in the Official Journal, eID schemes only become effectively available for cross-border authentication after almost 2 years. This duration is very long compared to the speed at which the identity market is developing and could deter private identity providers to enter such procedure. A vast majority of the members of the Cooperation Network consulted on their perception of the peer review procedure replied that the understanding of the **peer review and its scope** between Member States required clarification. As part of this evaluation, 39% of consulted members of the Cooperation Network were also of the opinion that the circumstances, formats and procedures for the pre-notification of eID schemes were not adequate. Member States raised concerns over the tendency in some peer reviews to go beyond scope with regard to the level of security scrutiny, rather than focus on an overall assessment of the eID schemes against the requirements of the Regulation and correct assessment of the Member State declared LoA of its pre-notified eID solution.

There is also no **uniform understanding on how to assess new and emerging technologies and innovative solutions**. Since 2018, there is an ongoing controversy among experts in the Cooperation Network about the security of mobile schemes, remote on-boarding solutions, biometric authentication and the associated best-practices and levels of assurance. These controversies and disagreements complicate peer reviews and in one specific case have delayed the conclusion of the notification procedure for over one year. Guidance documents have not been able to substantially improve these procedural weaknesses given that by September 2020 agreement between Member States' experts had not yet been found on guidance regarding levels of assurance and peer reviews despite discussions ongoing for around two years.

Another concern raised by Member States with regard to the peer review procedure is **the lack of legal value from the opinion**. As such, nothing prevents a Member State to notify an eID scheme

⁸⁴ Or citizens above a certain age.

⁸⁵ Estonia reaches a value above 100% because it also issues an eID to foreigners who do not live in Estonia.

at a higher level of assurance than the conclusion of the peer review performed by the member of the Cooperation Network. Such a situation would greatly disrupt the whole trust framework as Member States would be compelled to recognise such eID scheme.

There is a lack of common vision among Member States on the purpose of the peer review process: some are focussing on the technical details and implementation of the eID schemes while others are adopting a more risk assessment approach. There is an agreement that more resources should be dedicated to the issuance of guidance on understanding how to assess new technological developments (e.g. remote video solutions, biometrics, etc...).

Ensure that all consumers can benefit from the advantages of cross-border eID

In many cases, access to an eID scheme is linked to the residence status of the respective user. Currently, 41% of EU citizens don't have access to a notified and high level-of-assurance eID because their countries do not offer such a solution and they are unable to obtain an eID in another country.

One aim of the Regulation was to ensure that eID schemes notified under eIDAS would be used by public and private sectors to access online services across borders. In February 2021, 14 of the EU Member States have already notified at least one eID scheme and 2 Member States have pre-notified.⁸⁶ This means that half of the EU have not pre-notified or notified an eID scheme under eIDAS yet. This lack of availability of notified eID schemes limits the usage of notified eIDs by public and private sectors in Europe. Even for the notified eID schemes, there is a limited availability of services in practice. Not all public services that should have been accessible via the eIDAS framework can actually be accessed that way.

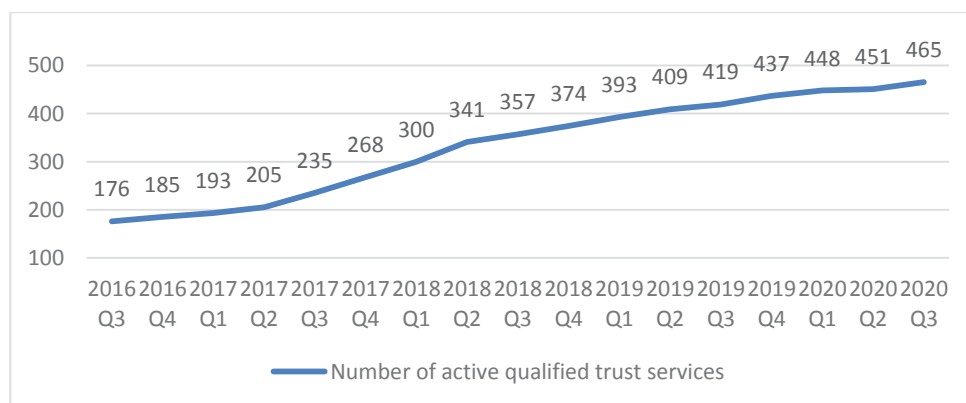
Trust services

Increase availability and take-up of cross-border and cross-sector trust services

While the availability of trust services refers to the number of services available across Europe, the take-up of trust services describes the actual usage of the different trust services. Both the availability and take-up of trust services in Europe have been increasing since the introduction of the eIDAS Regulation, however, there are differences among Member States and among different trust services, not least due to the prevalence of national requirements for the use of trust services in specific sectors.

The increased availability of services correlates with an increased number of trust services providers, as indicated by the entries on the EU Trusted List:

Figure 11 Evolution of the number of Qualified Trust Services (2016-2020)⁸⁷



⁸⁶ The United Kingdom notification of UK.GOV Verify is not included in this analysis.

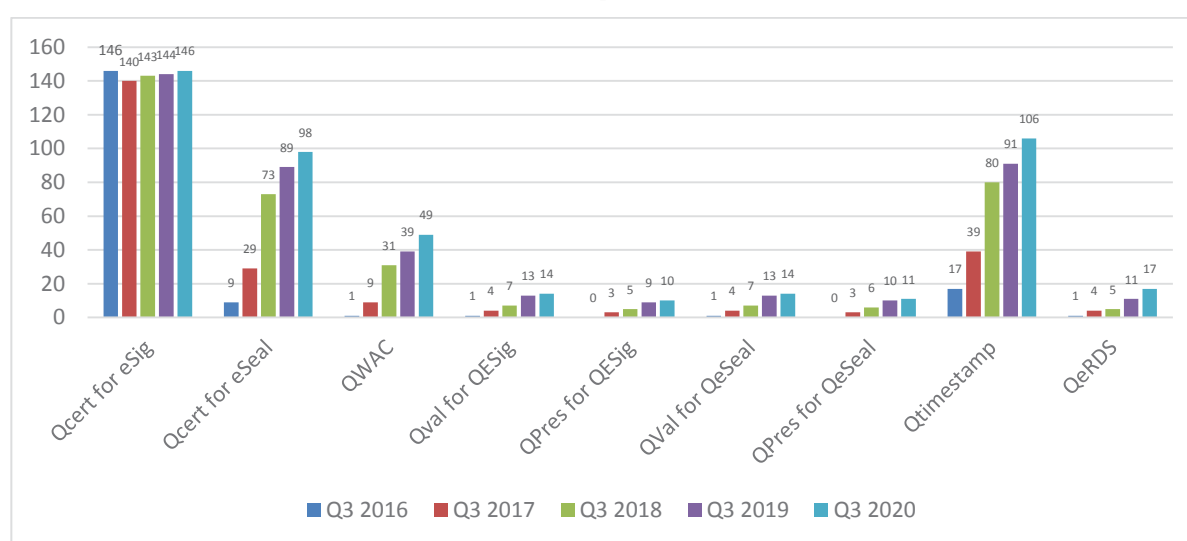
⁸⁷ Abstract from the TL Browser, see: <https://webgate.ec.europa.eu/tl-browser/#/>

Respondents to the OPC agreed that the eIDAS Regulation has increased the availability of electronic trust services in the EU as follows: eSignature (78%), eSeal (78%), and eTimestamps (73%). A majority of respondents furthermore agreed that the eIDAS Regulation had increased the availability of ERDS (51%).

With regard to their uptake, 77% of respondents to the OPC stated that they had already used electronic trust services, and 65% stated that they felt more comfortable and confident to use trust services now compared to five years ago. Still, 89% of respondents agreed that public administrations should make better use of electronic trust services in their contact with citizens and businesses.

In terms of the repartition of trust services, QeSignature, QeSeals and QTimestamps are the services mostly used. The number of QWAC, QeSeal, Preservation, QERD, QVal are significantly less in demand.

Figure 12 Repartition per type and evolution of the number of qualified trust services (2016 – 2020)⁸⁸



Ensure an optimal level and scope of governance for trust services

The eIDAS Regulation has set up a governance framework for trust services that includes supervisory bodies, conformity assessment bodies and trusted lists for trust service providers in Member States. A full description of the supervisory mechanism of trust services is presented in Section 3.2.

Respondents to the OPC were divided on the effectiveness of the governance framework and only 37% agreed that it was adequate.

The key governance issue raised by stakeholders concerns the **lack of harmonisation in conformity assessment** which resulted in different national approaches and a possible ‘race to the bottom’ where trust service providers may turn to the cheapest or least stringent certification scheme. Several stakeholders proposed to base accreditation on standards⁸⁹ in order to provide

⁸⁸ Abstract from the TL Browser. Q3 corresponds to an abstract on July 2nd each year. See: <https://webgate.ec.europa.eu/tl-browser/#/dashboard>

⁸⁹ Standard ETSI EN 319 403. ETSI, Certification Authorities and other Trust Service Providers, see: <https://portal.etsi.org/TB-SiteMap/ESI/Trust-Service-Providers>

more clarity to the CABs on how to assess qualified trust service providers. This opinion is shared by ENISA in a report published in May 2019.⁹⁰

Stakeholders also complain about **the lack of referenced standards** as foreseen in articles 24(1), 24(5), 28(6), 32(3), 33(2), 34(2), 38(6), 40, 42, 44(2) and 45 in order to allow for a more harmonised assessment of the functional requirements against appropriate technical and organisational standards.

Another issues raised by a number of stakeholders is the different approach of Supervisory Bodies regarding the **acceptance of remote identification methods** and their consideration as equivalent to “physical presence” as per article 24(1)(b) of the eIDAS Regulation given the absence of EU-level guidance with the associated risks of an unlevelled playing field and ‘race to the bottom’. At the same time, there is a growing demand to authorize remote identification for on-boarding of users given physical distance requirements as a result of the COVID-19 crisis. Supervisory Authorities are therefore calling for the harmonization of requirements with regard to remote identification.

Some supervisory authorities have also raised concerns regarding the **lack of supervision of non-qualified trust service providers**. Article 19(1) of the eIDAS Regulation requires that qualified and non-qualified trust service providers take appropriate technical and organisational measures to manage security risks. However, the absence of supervision obligations at EU level leads to a lack of market data and may result in non-reporting of security breaches by non-qualified TSPs.

The ENISA Article 19 Expert group also points to a **gap in the supervision of third-country trust services provided within the EU**. Trust services providers established in third countries providing trust services in Europe, e.g. for the provision of QWACs, rely on registration offices or “supporting services” in the EU which however are not supervised themselves. This may also be linked to a lack of common understanding for the concept of establishment (Article 17.3).

Need for the recognition of the forum of cooperation in the field of trust services

Article 18(1) of the eIDAS Regulation foresees that Supervisory bodies cooperate with a view to exchanging good practice, however no formal governance body has been established for this purpose similar to the Cooperation Network on eID. An informal forum of information exchange was created by ENISA to facilitate cooperation on security breaches following article 19 of the eIDAS Regulation.⁹¹ The focus of the group is to define technical details of incident reporting, ensure ad-hoc reporting about incidents, as well as an annual summary report. The decisions of this group are not binding.

Q3. To what extent has the Regulation met its general objectives?

Develop a digital single market for eID and trust services

The market for identity authentication and fraud solutions is set to grow from EUR 10.3 billion in 2018 to about EUR 23.6 billion by 2023 worldwide, with identity authentication making up a major part of this growth.⁹² In Europe, the identity verification market is expected to grow from EUR 1.23 billion in 2018 to EUR 3.71 billion by 2027.⁹³ eIDAS and the Connecting Europe Facility (CEF) programme have built a digital infrastructure across the EU that successfully supports

⁹⁰ ENISA, Towards global acceptance of eIDAS audits, May 2019, see: <https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits>

⁹¹ ENISA, Article 19 Expert Group workspace, see: <https://resilience.enisa.europa.eu/article-19>

⁹² BCG, A Great Digital Identity Solution Is One You Can't See, see: <https://www.bcg.com/en-be/publications/2019/digital-identity-solution-one-you-cannot-see>

⁹³ Intrado, Europe Identity Verification Market to 2027, see: <https://www.globenewswire.com/news-release/2019/11/04/1939959/0/en/Europe-Identity-Verification-Market-to-2027-Regional-Analysis-and-Forecasts-By-Component-Deployment-Organization-Size-End-user.html>

Member States and businesses to set up this infrastructure via a set of generic digital building blocks.

In the area of trust services, the eIDAS Regulation has enabled companies to develop their business cross borders. More than half of trust service providers consulted consider that the eIDAS Regulation enabled them to increase their customer base in the EU and 75% think that the eIDAS Regulation has resulted in an increased use of the trust services they provided.

Although the aggregated feedback of public and stakeholder consultations clearly confirm an important and positive contribution by eIDAS to the creation of a European market for trust services, the analysis of the eID market shows continuing fragmentation between public and private providers with limited take-up of eID/eIDAS in the private sector.

The World Economic Forum has identified the lack of commercial models for public-led eID schemes as a distinct gap in the digital identity landscape today.⁹⁴ At the moment, the absence of a common commercial model for eID including common rules on costs and liabilities lead to a fragmented eID market which is not attractive to private service providers. The current situation does not justify investments by service providers to connect to the eIDAS network:

- Member States set terms and conditions of access to eIDAS nodes at national level. In some cases access is free while in other cases investment costs are recovered. In addition, there is no obligation for Member States to accept cross-border authentication requests coming from private service providers.
- Cost recovery rates and procedures for the use of notified eID have not been set generally requiring individual contracts with service providers and different invoicing models and conditions.
- Private service providers miss information on the terms and conditions of their access to eIDAS nodes. In case they offer services at EU level only, there is no guidance to which national eIDAS node to connect;
- Fragmentation of the market and multiple conditions make it difficult for private service providers to build a business case based on connection to the eIDAS network and effective access to a critical mass of users.

A different path on national level has been followed by Nordic countries where public sector authorities purchase identity provision from the private sector (bankID). Each transaction is therefore a cost for the state budget, contrary to countries which have integrated eID as a publicly financed infrastructure. However, it is less straightforward for Member States to notify a private sector led eID scheme (e.g bankID) that the government does not fully control. For example, in all Member States banks have methods of authenticating their users. Some eID means can be used only in one bank, others across different banks, government and other private services.

Promote the interest and protection of end-users (citizens and businesses)

Trust service providers consulted were divided on whether the eIDAS Regulation adequately addresses data and privacy concerns (51% agreed with the statement while 29% disagreed). 19% of OPC respondents mentioned privacy concerns as a limiting factor for the use of eID and trust services.

The Future Trust research project⁹⁵ investigated to what extent the eIDAS Interoperability Framework should be adapted to comply with the high level of data protection introduced by the

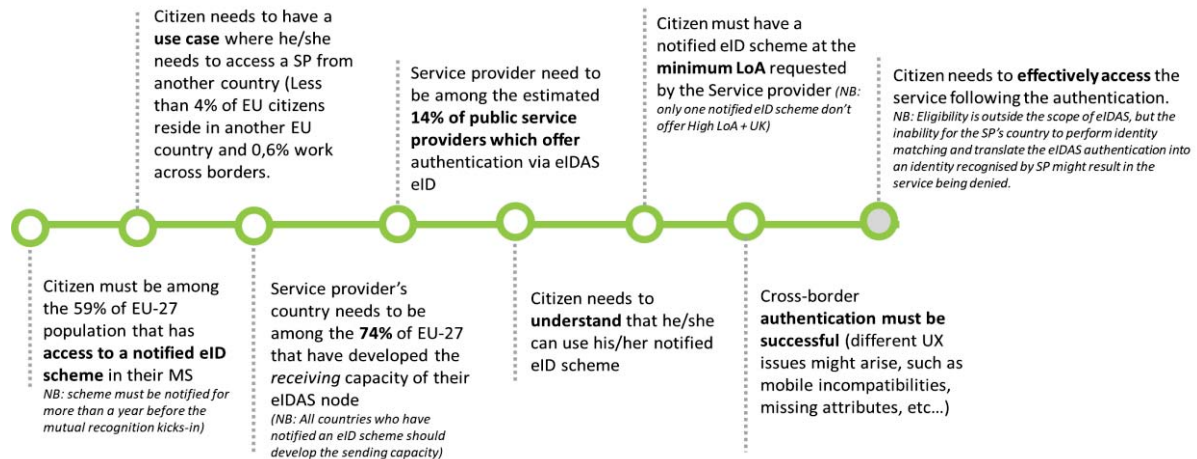
⁹⁴ World Economic Forum, A blueprint for Digital Identity, August 2016. See: http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

⁹⁵ Future Trust, Documentation of the Legal Foundations of Trust and Trustworthiness, 2018, see: https://docs.wixstatic.com/ugd/2844e6_b441a5f255f94cf78a7d4c890e2fe6aa.pdf

European General Data Protection Regulation (GDPR).⁹⁶ At the moment, when a user authenticates to a foreign online service, the whole eIDAS minimum dataset is automatically shared with the relying party. The study proposes a modification of the technical specifications in order to enable selective disclosure (e.g. sharing only the necessary attributes for the service) and pseudonymisation (e.g. tokenization of unique identifiers) of transmitted attributes.

The eIDAS Regulation foresees a minimum data set for legal persons. Only one Member States has notified so far an eID scheme for legal persons (NL – eHerkenning). However, in general, the number of schemes dedicated to legal persons in Europe is rather limited. We assume that the lack of notification is due to the minimal availability of such schemes and not due to a blocking factor linked to the disposition of the eIDAS framework.

Figure 13 Overview of limiting factors to the uptake of eIDAS eID in Europe



Overall, the eIDAS framework has proven ineffective to ensure that EU citizens have access to a secure means of eID that can be used cross-border. This is due to a number of key limiting factors and multiple conditions that must be met to ensure successful cross-border authentication. The current technical and legal set-up is too complex and limited to too few use cases, while the needs and business cases of private sector service providers are not captured. In the area of trust services, the eIDAS Regulation has proven generally effective, in particular with regard to eSignatures, eSeals and eTimestamps.

5.2 Efficiency

Q4. Did the regulatory intervention create any additional costs and benefits for targeted stakeholders?

Electronic identification

Concerning eIDs (Article 6 to 12), the main purpose of the Regulation is to ensure that national eID schemes issued in one country can be used in any other. This implies the need to coordinate a series of activities, including communication and verification of information performed by different stakeholders. The key stakeholders includes:

- **National authorities and eIDAS node operators** responsible for ensuring correct performance of the eIDAS infrastructure;
- **eID providers** responsible for issuing the electronic identification means;

⁹⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, see: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

- **Service providers (using eID)** offering online services that rely on eID for cross-border authentication according to Article 7 (eligibility for notification), Article 8 (assurance levels) and Article 11 liability of the eIDAS Regulation.

Table 3 Mapping of costs for eID stakeholders

	Administrative burdens	Substantive compliance	Enforcement costs
National authorities and eIDAS operators	<ul style="list-style-type: none"> • Mutual recognition of eID nodes • Notification of eID schemes (and pre-notification) – including preparation for peer review • Peer review of other MS schemes • Communication security breaches • Cooperation and interoperability with other MS 	<ul style="list-style-type: none"> • Operational costs (node operators) • Costs entailed by the assurance levels • Costs due to adaptation of national regulatory framework (if needed) • Liability costs in case of security breaches 	<ul style="list-style-type: none"> • Supervisory of private eID providers • Compliance certifications of private eID providers
eID providers	<ul style="list-style-type: none"> • Notification of eID schemes (and pre-notification) – including preparation for peer reviews 	<ul style="list-style-type: none"> • Interface with national infrastructure/technical interoperability • Technical costs related to level of assurance • Liability costs in case of security breaches 	
Service Providers		<ul style="list-style-type: none"> • Specific interface with national infrastructure – connector • Adaptation costs 	

Administrative burdens and costs

For national authorities and eIDAS node operators:

- **Mutual recognition obligations (Article 6):** These obligations require Member States to recognise notified electronic identity issued in another Member State. The main costs relate to obligations set in Article 7 identifying eligible entities to issue an electronic identification scheme and to Article 9 setting information obligations that must be provided in the notification process (par. 1) and obligations regarding the communication of eID schemes that are no longer valid (par. 4).
- **Cooperation and interoperability (Article 12):** – ID EU 2015/296. Costs entailed by the participation of Member States to the interoperability framework (exchange of information, good practices, peer review of electronic identification schemes, etc.).
- **Notifications of security breaches and suspension or revocation of eID schemes**

For eID providers:

For eID providers, the main administrative burden relates to the notification process.

Substantive compliance costs

Substantive compliance costs include investments and expenses to be covered by businesses and citizens to comply with obligations or requirements.

For national authorities and eIDAS node operators:

Substantive compliance costs are generated by the following procedures:

- **eIDAS node Management:** Annual operating costs (both internal costs and outsourcing costs) that Member States Agencies and node operators incur to manage the eIDAS node.

- **Security:** Security is the most relevant source of cost since notified electronic schemes must comply with the levels of Assurance as defined in Article 8 “Assurance levels of electronic identification schemes”. These levels of assurance (low, substantial and high) are linked to requirements which in practice require investments into certain levels of technology.
- **Regulatory adaptation Costs:** These costs incur in the adaptation of national regulatory frameworks such as national regulatory provisions on the use of electronic identities issues in other Member States for the access of national public services.
- **Liability Costs (Article 11):** Liability costs may arise to cover security breaches as Member States are liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations stated in the eIDAS Regulation.

For eID providers:

- **Connection Costs:** Operational costs for the eID provider to connect to the national Node.
- **Investment in Technology:** eID must ensure a certain level of security or assurance. Investment in technology is required to ensure assurance levels are met;
- **Liability costs in case of security breaches:** Also eID providers, are liable in case of security breaches according to Article 10.

For Service Providers:

The eIDAS Regulation does not foresee costs for service providers which can access the network free of charge. However, adaptation costs may incur for the purpose of identity reconciliation in external / national databases for the purposes of the service it provides.

Enforcement costs

Enforcement costs are associated with activities such as monitoring, enforcement and adjudication. For these activities, the eIDAS Regulation mandates national authorities that, in cases of security breach, may suspend or revoke electronic identity schemes. In addition, in Member States where eID/eIDAS providers are private, costs incur for the purpose of their supervision and issuing of certifications of compliance.

Benefits

National authorities and eIDAS node operators

Direct benefits of the eIDAS Regulation for national authorities and eIDAS node operators are difficult to identify and quantify. In qualitative terms, national authorities and eIDAS node operators consulted, underlined that cross-border usage of eIDs and exchange of information and best practices can increase the efficiency in the implementation process of new technologies, thereby resulting in administrative cost-savings for public services.

eID Providers

Benefits result from the reputational value associated with compliance with the high standards of EU Regulation, which in turn improves the market position of a private provider and generates potential benefits in terms of revenues and access to capital. In addition eIDAS can generate indirect benefits associated with legal compliance with requirements in the area of financial services, AML, privacy and cybersecurity.

Service Providers

Administrative savings are generated by the reduced front-desk costs for service providers, which is also reflected in time-saving for end-users (both in terms of the process to acquire an additional ID in another country and the need to be present physically). For private service providers, a source of benefit is the larger market base provided by cross-border use as more users can access digital

services from abroad. In addition, interviewees underlined the benefits of increased security and assurance, particularly in certain countries. Key benefits of trusted eID provision to private service providers in terms of liability management and cost-savings through the outsourcing of identification and authentication could not be quantified given the insufficient take-up of eID / eIDAS with private sector service providers.

Trust services

The analysis of costs related to Trust Services focuses on the effects of their cross-border recognition ensured by the eIDAS Regulation. The stakeholder mapping below provides an overview of the entities for which the eIDAS Regulation envisages specific requirements or duties (and the related articles from the eIDAS Regulation) that are generating costs.

Table 4 Mapping of costs for Trust Services stakeholders

	Administrative burden	Substantive compliance	Enforcement costs
Supervisory body	<ul style="list-style-type: none"> Informing national body responsible for trusted lists Reporting to European Commission Informing Data Protection Authorities 	<ul style="list-style-type: none"> Cost for reciprocal assistance provision 	<ul style="list-style-type: none"> Analysing conformity assessment reports Carrying out audits (borne by QTSPs) Granting or withdrawing qualified status Requiring (Q)TSP to remedy failures
Qualified TSP	<ul style="list-style-type: none"> Qualification procedure Communication of security breaches Audit costs 	<ul style="list-style-type: none"> Technical expenses Physical assets Liability costs 	
Non-Qualified TSP	<ul style="list-style-type: none"> Communication of security breaches 	<ul style="list-style-type: none"> Technical expenses Physical assets Liability costs 	N/A

Administrative burden and costs

Supervisory Authorities

Supervisory activities generate two types of costs: enforcement costs and administrative costs related to reporting and cooperation obligations. For supervisory authorities, the following administrative costs may incur:

- Cooperation with other supervisory bodies and assistance in accordance with Article 18;
- Information on breaches of security or loss of integrity in accordance with Article 17.4(c);
- Activity reporting to the Commission in accordance with paragraph 6 of Article 17.4(c);
- Cooperation with data protection authorities and information on audits of qualified trust service providers where personal data protection rules appear to have been breached;
- Information on updates to the national trusted list referred to in Article 22(3) unless the list is managed by the supervisory body.

Supervisory authorities ensure that market operators (TSPs and QTSPs) operate in compliance with relevant regulations and meet the requirements of the eIDAS Regulation. In this context, costs related to the following enforcement activities may incur⁹⁷:

- Ex ante and ex post supervisory activities to ensure that QSTPs and the qualified trust services that they provide meet the requirements laid down in this Regulation;

⁹⁷ Costs may include adjudication costs (e.g. the costs related to the recognition of the status of qualified TSP), monitoring costs and enforcement costs (e.g. the costs related to the identification, in case of lack of compliance by a QTSP, of the measures that the operator must implement to meet compliance requirements). Costs of audit by CAB and AB are borne by QTSPs.

- Action taken in relation to non-qualified trust service providers established through ex post supervisory activities in case those TSPs or the trust services they provide do not meet the requirements laid down in this Regulation;
- Analysis of conformity assessment reports referred to in Articles 20(1) and 21(1);
- Audits of the qualified trust service providers;
- Granting of qualified status to trust service providers and to the services they provide and withdrawal of this status
- Verification of follow-up to termination plans in cases where the qualified trust service provider ceases its activities;

Trust Service Providers

Obtaining the qualified status entails administrative costs for Trust Service Providers (TSPs):

- To become a QTSP, the trust service provider must undergo an assessment by a CAB and then file a request to the Supervisory body;
- Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body and must communicate the results to the Supervisory Body (Article 20.1);
- In case of failure to meet the requirements, the QTSP must implement the remedies within the timeframe determined by the Supervisory body.

Substantive costs will also be incurred for TSPs to take appropriate technical and organisational measures to manage security risks associated with the trust services they provide. There are no additional direct substantive costs for non-qualified trust services.

For QTSPs there are also substantive costs related to fulfilling overall requirements as specified in Article 24 and related to:

- registration of third parties;
- employment policies;
- financial resources necessary for liability management;
- use of specific trustworthy technology;
- measures in case of data theft;
- record keeping;
- preparation and update of termination plans;
- appropriate and lawful processing of personal data;
- keeping a certificate database.

Benefits

The results of the consultation process suggests that a majority of respondents believe that significant benefits have been achieved. Over 70% of respondents consider that the trust service part of the eIDAS Regulation contributed to cost savings, time savings, legal certainty and simplification of administrative procedures.

Trust Service Providers

Trust Service Providers register benefits in the form of revenue due to the provision of trust services in other EU countries and an extension of market base. This is also linked to a reputational increase and better access to finance due to compliance with the high standards of eIDAS Regulation. For Qualified Trust Service Providers these benefits generally have greater impact also due to an increased number of use-cases for qualified trust services.

Supervisory Bodies, Conformity Assessment Bodies and Accreditation bodies

For Supervisory Bodies, Conformity Assessment Bodies and Accreditation bodies, benefits relate to harmonised standards, clear functions, and simplified supervisory processes compared to a highly fragmented setting prior to the implementation of the eIDAS Regulation. Firstly, mutual exchange of information between bodies in different countries makes inspection, qualification, and assessment procedures faster and cheaper and best-practice exchange increases efficiency and enforcements capabilities. Secondly, trust service providers that undergo a procedure in one country do not have to repeat it in other Member States.

Q5. How proportionate is the amount of costs and benefits to cost and benefit items? How are they broken down? How do they compare across different stakeholder groups?

To respond to this evaluation question, costs and benefits identified were quantified and monetized following the data collection process described in Annex 3. The quantification process is based on a series of assumptions and limitations, as outlined in the methodology section. The stakeholder selection has been elaborated to build a representative sample of the entire eIDAS stakeholders, cutting through different geographical areas and country sizes in the 31 countries under analysis. The sample of quantitative data was extended to 124 stakeholder responses collected through the in-depth interviews and survey. Nevertheless, only 643 responses, equal to 51.6% of the sample, were containing numerical values that have been used for the final estimates. Therefore, the representativeness of the data is constrained and the figures should be regarded as indicative only. In particular, respondents found it particularly difficult to estimate the direct benefits of the Regulation, for which a quantification was only possible for trust service providers.

Table 5 Results of the data collection

Stakeholder group	Survey	Targeted interviews	Total sample	Data provided
National policymakers	19	6	25	10
eID providers	4	5	9	4
Service Providers	4	3	7	3
AB, SB, CAB	34	6	40	23
TSP (Q and non-Q)	36	7	43	24
TOT.	97	27	124	64

The overall results of the quantification and monetization process **per average stakeholder** is reported in the table below. The figures report the ranges of costs and benefits that were reported by participants. Variance is due to the different structures and degree of implementation of eID in some countries and, for trust services, the size of the company, the range of their services and their market presence.

Table 6 Data collection results: range values, in EUR (n sample)

Stakeholder	Initial costs	Recurring administrative costs	Recurring technical costs	Benefits
National policymakers	40,000 – 2,300,000 (8)	10,000 – 500,000 (7)	30,000 - 650,000 (9)	N/A
eID providers	10,000 – 4,500,000 (3)	100,000 – 2,000,000 (4)	75,000 – 2,750,000 (3)	N/A
Service providers (eID)	55,000 – 230,000 (3)	25,000 – 1,000,000 (3)	N/A	N/A

AB, SB, CAB	N/A	0 – 1,550,000 (23)	N/A	N/A
Q TSP	50,000 - 10,000,000 (19)	3,000 – 4,750,000 (17)	N/A	0 – 20,000,000 (9)
non-Q TSP	N/A	3,000 – 4,750,000 (17)	N/A	10,000 (2)

The overall data dispersion and the limitations to the sample for each figure suggest caution in data analysis. Action needs to be taken to improve data robustness. Based on current data availability and under the assumption that the sample for each stakeholder group is representative of the population, the average costs and benefits for each individual stakeholder were calculated. As adjustment measures, the central tendency of the data and the data dispersion was considered, excluding outliers when possible. The main output measure are the average costs per organisation, completed by the average FTEs (“full-time equivalent”) dedicated to eIDAS activities. The quantification of benefits was only possible for trust service providers.

In general, the costs and benefits generated by the eIDAS Regulation are not evenly distributed across all stakeholders. As expected, the costs are mainly borne by public authorities, while benefits have been identified mostly for users and market operators.

Electronic identification

Table 7 *Quantification of costs and benefits for the average national authority/eIDAS node operator*

Stakeholder	Indicator	Figures		
National policymakers	Average number of Full-time Equivalent (FTE - as a measure of how many employees (in full-time equivalents) are dedicated to activities generated by the eIDAS Regulation)	4		
	Initial costs	750,000€		
	Recurring administrative costs 180,000€	Share for notification process of eID schemes	30%	54,000€
		Share for peer review process of other countries' eID schemes	25%	45,000€
		Share for cooperation and communication activities with other Member States and the European Commission	20%	36,000€
		Share for other administrative activities not included above but related to the duties of the eIDAS Regulation	25%	45,000€
	Recurring technical costs	225,000€		
Benefits	N/A			

Costs

The average annual administrative cost for **national authorities and eIDAS node operators** amount to EUR 180,000. The largest share of this cost relates to the notification process of eID schemes (30%) and almost half of this amount (45%) refers to costs for the peer review process of other eID schemes as well to costs for cooperation and communication activities with other Member States and the European Commission. One quarter of the annual average administrative costs (EUR 45,000) relates to other administrative activities. National authorities and eIDAS node operators also incur annual recurring technical costs for an average amount of EUR 225,000 (such as annual fees to external providers of technology services). Initial costs to set up the eIDAS node and the administrative procedures to access the eIDAS network, have been reported as amounting to EUR 800,000 on average.

Table 8 Quantification of costs and benefits for the average eID Provider

Stakeholder	Indicator	Figures		
eID Providers	Average number of Full-time Equivalent (FTE - as a measure of how many employees (in full-time equivalents) are dedicated to activities generated by the eIDAS Regulation)	5		
	Initial costs	275,000€		
	Recurring administrative costs 220,000€	Share for notification process of eID schemes	60%	132,000€
		Share for peer review process of other countries' eID schemes	20%	44,000€
		Share for other administrative costs	20%	44,000€
	Recurring technical costs	235,000€		
Benefits	N/A			

In the case of **eID providers**, as reported in the table above, the initial costs amount - on average – to EUR 270.000. Regarding the annual recurring administrative costs, the largest share (60%) relates to the notification process of eID schemes, while a significant share of 20% relates to the peer review process of other eID schemes. The annual recurring technical costs are almost at the same level as for national authorities and eIDAS node operators (EUR 235,000).

Table 9 Quantification of costs and benefits for the average Service Provider

Stakeholder	Indicator	Figures		
Service Providers	Initial costs 125,000€	Share for administrative tasks and paperwork	50%	62,500€
		Share for technical requirements	35%	43,750€
		Share for other costs not included in administrative costs and technical requirement	15%	18,750€
	Recurring total costs for the connection to the national node	31,000€		
	Benefits	N/A		

The table above reports the figures for **service providers**. The initial costs service providers incur are significantly lower than for other stakeholder groups. 50% of these costs refer to administrative tasks, 35% relates to technical requirement and 15% relates to other costs. On the other hand, service providers need to cover recurring annual costs in relation to their connection to the national node, amounting to EUR 31,000 on average.

Trust services

Table 10 Quantification of costs and benefits for the average AB, CAB, and SB

Stakeholder	Indicator	Figures		
Accreditation, Conformity Assessment, and Supervisory Bodies (AB, CAB, and SB)	Full-time Equivalent (FTE - as a measure of how many employees (in full-time equivalents) are dedicated to activities generated by the eIDAS Regulation)	3		
	Recurring administrative costs 120,000€	Share enforcement activities (analysing conformity assessment reports, carrying out audits, granting or withdrawing qualified status, requiring (Q)TSP to remedy failures) pertaining Article 17.4 of the eIDAS Regulation	60%	72,000€
		Share of administrative procedures (informing national body responsible for trusted lists, reporting to European Commission, informing Data Protection Authorities, etc.) pertaining to Article 17.4 of the eIDAS Regulation	15%	18,000€

		Share for reciprocal assistance provision (Article 18) of the eIDAS Regulation	5%	6,000€
		Share due to other activities not covered by the activities mentioned above	20%	24,000€
	Initial costs		N/A	
	Benefits		N/A	

For **Accreditation Bodies, Conformity Assessment Bodies, and Supervisory Bodies (AB, CAB, and SB)**, the main share of costs relates to various administrative activities and procedures, while initial costs could not be quantified.

60% of recurring administrative costs are allocated to enforcement activities (analysing conformity assessment reports, carrying out audits, granting or withdrawing qualified status, requiring (Q)TSP to remedy failures) pertaining Article 17.4 of the eIDAS Regulation. The rest of recurring administrative costs relate to:

- 15% to other administrative procedures (i.e. informing national body responsible for trusted lists, reporting to European Commission, etc.);
- 20% to reciprocal assistance provision (Article 18) of the eIDAS Regulation;
- 20% to other enforcement activities.
- Recurring technical costs amount to an average of EUR 225,000.

Table 11 Quantification of costs and benefits for the average Qualified TSP

Stakeholder	Indicator		Figures		
Qualified TSP	Total costs of qualification (costs incurred in order to qualify, be granted, and maintain the status of qualified trust service provider, according to the eIDAS Regulation) 800,000€	Share dedicated to administrative tasks (i.e. cost of personnel filing the paperwork, audit procedure, conformity assessment, other)	45%	360,000€	
		Share for technical expenses (i.e. investments in new technologies, physical assets which, technical consulting support due to the requirements of the qualification)	50%	400,000€	
		Share for other expenses	5%	40,000€	
	Recurring costs - Overall yearly estimate of the recurring extra-costs compliant with the eIDAS 750,000€	Share due to administrative tasks (i.e. paperwork)	40%	300,000€	
		Share dedicated to technical expenses ex Article 19 (i.e. recurring investments physical assets, in software updates, etc.)	35%	262,500€	
		Share due to storage of OCSPs (or other storage costs)	5%	37,500€	
		Share due to procedures of notification of security breaches to the supervisory authorities and users	10%	75,000€	
		Share due to other activities not covered by the activities mentioned above	10%	75,000€	
	Benefits			2,711,000€	

Table 12 Quantification of costs for the average Non-Qualified TSP

Stakeholder	Indicator		Figures	
Non-Qualified	Recurring costs - Overall	Share due to administrative tasks (i.e. paperwork)	40%	300,000€

TSP	yearly estimate of the recurring extra-costs compliant with the eIDAS 750,000€	Share dedicated to technical expenses ex Article 19 (i.e. recurring investments physical assets, in software updates, etc.)	35%	262,500€
		Share due to storage of OCSPs (or other storage costs)	5%	37,500€
		Share due to procedures of notification of security breaches to the supervisory authorities and users	10%	75,000€
		Share due to other activities not covered by the activities mentioned above	10%	75,000€
Benefits			10,000€	

Trust Service Providers: QTSP have significantly higher costs than non-Qualified TSPs. Costs can be differentiated in two main categories:

- One-time costs incurred to reach and maintain qualified status amount to an average of EUR 800,000, of which 45% are dedicated to administrative tasks and 50% relate to technical costs (i.e. investments in new technologies, physical assets).
- Annual recurring compliance costs of an average of EUR 750,000, of which 40% for administrative tasks, 35% for technical expenses (i.e. recurring investments physical assets, in software updates, etc.), 5% for storage of OCSPs⁹⁸ and 20% to notify security breaches.

For non-qualified TSPs, only recurring compliance costs apply (amounts and shares are identical with the ones for Qualified TSP).

Benefits

The average benefit per company as reported by QTSPs is around EUR 2.7 million⁹⁹. QTSPs¹⁰⁰ declare a significantly higher amount than non-qualified TSPs (EUR 2,711,000 and EUR 10,000 respectively), which appears partially justified by larger market share¹⁰¹.

Q6. To what extent have the aggregate costs of the Regulation been justified and proportionate given the aggregate benefits achieved?

From a qualitative perspective, most of the interviewed stakeholders pointed out that the eID framework still has to demonstrate its full potential:

1. national agencies in charge of eID are still in the process of fully integrating with the eIDAS network;
2. take-up and use of eID by citizens is expected to grow;
3. availability of service providers linked to the eID / eIDAS network is equally expected to grow.

Therefore, investments made by **national agencies and eID providers** currently outweigh the benefits of cross-border use of national eIDs to access service providers in another country. The

⁹⁸ Online Certificate Status Protocol

⁹⁹ Only few responses to this question have been received and there are considerable differences in market size and company size.

¹⁰⁰ The main benefits are: incremental revenues due to the provision of trust services in other EU countries and larger market base; eIDAS compliance increases the reputation of TSPs on the market with potential benefits in terms of revenues and access to capital markets; incremental revenues due to the possibility for a company to access use-cases where only QTSPs are allowed; and increased demand for QTSPs when mandated for the use in public procedures.

¹⁰¹ Limitations apply – see previous footnote.

numbers of this type of transactions are still not consistently monitored, nevertheless it is expected that benefits will increase with a growing number of services connected. In addition, as reported by a private eID provider, if access to private service providers would be generally available, the potential market value would be extremely high as fees could be charged by eID providers.

For **cross-border eID users**, the possibility of using a national eID certainly represents an important reduction of administrative burden.

For **trust services**, stakeholders report that the administrative burden caused by the eIDAS Regulation is significantly outweighed by the cost reductions resulting from the cross-border availability of the services and the absence of requirements at national level.

Electronic identification

The following aggregate costs for eID stakeholders have been estimated as follows:

- *Member States*: Total annual recurring cost of EUR 12,555,000 and total initial set-up costs of EUR 23,250,000¹⁰².
- *eID providers*: overall recurring costs for eID providers amounts to an estimate of EUR 14,560,000 while overall initial costs are estimated at about EUR 8,800,000¹⁰³;
- *Service providers*: The total number of active (public) service providers is estimated at 6,200. Consequently, a theoretical aggregate cost of EUR 191,000,000 to service providers can be estimated¹⁰⁴.

Trust services

The aggregate costs for trust services stakeholders are estimated as follows:

- *Accreditation, Conformity Assessment, and Supervisory Bodies*: Recurring annual costs estimated to EUR 8,880,000 (31 supervisory bodies, 31 national accreditation bodies, and 12 conformity assessment bodies).
- *Qualified Trust Service Providers*: Aggregated annual costs amount to EUR 143,250,000, while the market costs of qualification amount to EUR 152,800,000, and aggregate annual benefits to EUR 517,822,413. (Based on input from 191 qualified trust service providers). These figures point to important net cost savings.
- *Non-qualified Trust Service Providers*: Annual costs are estimated at EUR 7,500,000 and the benefits to EUR 100,000 (based on the number of QTSP/TSP ratio). Overall, for non-qualified trust service providers, costs outweigh benefits.

Q7. Are there opportunities to simplify the legislation or reduce unnecessary regulatory costs without undermining the intended objectives of the intervention?

Electronic identification

The vast majority of stakeholders agreed that although eID/eIDAS was designed to also offer access to the private sector in addition to facilitating cross-border public services, there is still

¹⁰² The number of national authorities and eIDAS node operators (EU, the UK, Liechtenstein, Norway, and Iceland) used to estimate the overall market costs is 31. Nevertheless, as explained in the methodology section, not all countries have operational receiving and sending nodes in places. Nevertheless, for the purposes of this aggregate estimate we assume that all nodes are active. While this is not necessarily true at the time of the calculation.

¹⁰³ The number of total notified eID schemes as of September 2020 amounts to 20 provided by 32 public and private providers.

¹⁰⁴ Costs for service providers can be extremely variable depending on the complexity of the integration of the public service with the node. The number of active service providers accepting eID from other countries was estimated based on the consultation activities where each Member State provided a number. However, here is a strong selection bias as only larger service provider participated in interviews while the overall number of service providers also include smaller entities (e.g. municipalities) for which much lower costs are likely.

considerable room for improvement. Key issues discouraging private sector uptake include uncertainty costs:

- There is uncertainty regarding costs and benefits of providing and using eID schemes by private service providers as rules are not harmonised;
- There is a lack of rules and principles that would unambiguously define the rules for using eIDAS eID schemes in private services;

Several private eID providers consider that the costs of notification are balanced by potential benefits and national regulatory requirements rather than clearly identifiable market advantages.

To overcome these obstacles, stakeholders suggested to:

- increase information and awareness campaigns on the benefits of the eIDAS Regulation for specific stakeholder groups in order to increase the number of end-users and take-up by private service providers;
- provide easy and open access to eID schemes and systems in order to reduce the costs of the private sector when using them, as a first step to re-design the original purpose of eIDAS and shift its focus to support and facilitate the private sector;
- streamline and simplify the notification procedure.

For national authorities and eIDAS node operators, the most burdensome issue is the update of the national eIDAS node's connections to other nodes as this procedure is not centralised by the Commission but left to individual nodes. On the other hand, in case of a security breach, the two nodes involved have to align their respective log procedures in order to identify the transaction that effectively is object of the security breach, which is a complicated and time-consuming procedure. Considering that each node is upgraded at least once per year, some respondents argued that centralization of the process might improve its cost-effectiveness as every time that a node proceeds with an update, other nodes are automatically updated.

Remedies for the problem of identity matching are also suggested: National authorities and eIDAS node operators suggest a centralized repository of identities so that the public service provider could access a common repository for automatic matching.

Trust services

With regards to the costs and benefits for trust service stakeholder groups, the following main areas for corrective action were identified:

- Given that audit procedures and technical requirements imposed on trust service providers vary, greater coordination and harmonization of the supervisory procedures foreseen in Article 20 of the Regulation would increase market efficiency and reduce costs;
- The eIDAS Regulation does not ensure a comparable security level across the EU for QTSPs as the practice of conformity assessment bodies is not sufficiently aligned. This risks market distortion and a 'race to the bottom' since the market is likely to reward conformity assessment for the lowest price and the least requirements. Greater harmonisation can be achieved by detailing the provisions of Articles 19(1) and 24 of the eIDAS Regulation.
- Consumer awareness campaigns could promote the advantages of qualified trust services and increase market benefits.

5.3 Relevance

This section assesses whether the objectives of the eIDAS Regulation still address the present needs. It also identifies any discrepancies between objectives and problem drivers identified in the initial impact assessment and changes in circumstance.

Q8. To what extent do the initial objectives still correspond to the current needs and concerns?

The eIDAS Regulation identified four main problems at EU level: (i) the lack of cross-border and cross-sector interoperability regarding digital identity and trust services, (ii) the lack of trust in digital transactions, (iii) the lack of legal certainty with regard to the use of digital trust services compared to traditional paper-based solutions and (iv) the limited use of online public and private services.

In the field of **electronic identity (eID)**, the eIDAS Regulation established mutual recognition and acceptance of notified eID schemes. In the field of **trust services**, the eIDAS Regulation created a European internal market for trust services ensuring that these solutions have the same legal status as their paper-based equivalents. The overall objectives were to ensure the interoperability of such solutions at the EU level, to reduce administrative burden, to unlock the potential of electronic transactions for online public and private services.

Electronic identification

The need for identifying citizens in an online environment has sharply increased with the massive development of online public and private services. Digital services are becoming the norm and the preferred option of EU citizens to interact with their administration or private service providers.

The market development proved that the objectives of the Regulation have become – if anything – more pressing: a problem exacerbated by the COVID-19 crisis. While the Regulation initially set out to boost the use of online public and private services, the crisis made access to eID indispensable to all citizens throughout Europe for interaction with the public sector and in a large field also the private sector. This necessitates trustworthy digital transactions, legal certainty with regard to the use of digital trust services and cross-border, and cross-sector interoperability of digital identity and trust services.

Today, not all EU citizens have the possibility to obtain an eID scheme issued or endorsed by their national government and notified under the eIDAS Regulation. In the meantime, the private sector has developed own eID solutions.

The Fintech industry is especially keen on creating clearer rules for the recognition of remote identification and on-boarding of their clients to comply with the European Union's rules on anti-money laundering. Today rules differ and some countries impose more stringent requirements than others, requesting e.g. synchronous video chat (natural to natural person conversation) while others require only off-line pictures or videos for similar use-cases. These different national approaches result in telecoms and financial institutions being subject to different rules regarding remote identification across Europe.

Recently, the concept of Bring Your Own Identity (BYOI) has emerged, where users can select and use an eID of their choice either self-managed or provided by a third party. Social media platforms (such as Facebook, Google or LinkedIn), telecom operators, utility companies, universities and banks have developed such identities. They offer convenience to users who may reuse the same eID created to access social platforms or online banking to access other online services and in some countries even public services as some of these eID can be linked to legal identities following advanced verification processes.

The European Consumer Organisation (BEUC) support the idea that platforms operating in Europe should use eIDAS-certified identification mechanisms to verify the legal identity of users, notably

on marketplaces.¹⁰⁵ The verification of the legal identity of users would increase trust, notably reducing the possibility for fake reviews or ill intended sellers.

The current eIDAS framework focusing on notified eID schemes by EU Member States does not address the increasing need to offer all EU citizens with an easy to use and secure eID solution.

In a recent Eurobarometer on the attitudes towards the impact of digitalization on daily lives, 70% of EU citizens responded that they use a username, or email address and password to identify themselves when accessing online services in their daily life. 29% use their social media account.¹⁰⁶ Among these respondents, three quarters would like to know how their data is used when they authenticate to a website via their social media account.

The large majority of these eID solutions are currently not covered by the eIDAS Regulation. Citizens and businesses cannot compare the security and level of assurance that these different digital identity solutions provide. The absence of a systematic link between these digital identities and a verified (legal) identity also creates opportunities for fraud and cybersecurity threats. It is also difficult for the users to control the disclosure of personal information when using such identity solutions. The acceptance of these digital identity solutions by service providers is also highly fragmented, which means that citizens in practice need to own multiple identity schemes to prove their identity online. A large majority of EU citizens would like to have access to a single secure digital identity that they could use to access online services.¹⁰⁷ Finally, there is no seamless portability of attributes owned by users (e.g. ID attributes, driving license attributes, professional and educational degrees, passport ...) with the service provider of their choice, limiting the creation of innovative services around digital identities.

Moreover, as pointed out in the section on external coherence, the SDGR and the eIDAS Regulation are mutually reinforcing in their intervention logic. If users cannot digitally provide necessary evidence and thereby complete public service procedures cross-border online, they will have little demand to access it in the first place. SDGR, will provide the relevant obligations in this respect and thereby fill a gap that significantly damped demand for cross-border use of eID as provided by by eIDAS. Far from being outdated, the fundamental intervention logic for eID under eIDAS still holds and will leverage on the effects, for example, of the SDG from 2023 on.

In terms of security, stakeholders have raised concerns regarding the widespread use of biometrics for identity verification and authentication. At the moment, this has not been accompanied by an increased level of scrutiny at EU level despite the sensitiveness of the data at stake.¹⁰⁸

Trust services

For trust services, the market has developed positively according to predictions. The objectives of the eIDAS legal framework remain relevant to reduce market fragmentation by ensuring cross-border and cross sector interoperability by means of adopting common standards.

¹⁰⁵ BEUC, Ensuring consumer protection in the platform economy, October 2018, see:

<https://www.beuc.eu/publications/ensuring-consumer-protection-platform-economy/html>

¹⁰⁶ Eurobarometer 503, Attitudes towards the impact of digitalisation on daily lives, December 2019, see: <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2228>

¹⁰⁷ Eurobarometer 503, Attitudes towards the impact of digitalisation on daily lives, December 2019, see: <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2228>

¹⁰⁸ There is a lack of guidance on how to e.g. consider biometrics to assess level of assurances in eID/eIDAS described in the section on effectiveness.

Impact of COVID-19 pandemic

The Covid-19 pandemic has massively affected the European economy and society. As EU Member States implemented lockdowns, both public and private services moved their activities to digital by default and reduced - if not completely halted - interactions based on physical presence. Several countries have had to postpone election dates due to the absence of remote identification solutions. As a result, the need to rely on secure digital transactions and remote online identification has surged and the importance of secure electronic identification linked to online public services has become clear.

In case of trust services, the use of electronic signatures has allowed businesses and administration to continue sign contracts, invoices, and other legal documents. The pressure to maintain economic activities despite lockdown measures has pushed some countries to remove remaining obstacles to the full digitalisation of some procedures. In France, a specific decree has been adopted in April 2020 authorising the signature of notarised deeds at distance, while a physical presence was initially required.¹⁰⁹ In parallel, the demand for trust services notably eSignatures has increased exponentially. For example, Oodrive, the parent company of the qualified trust service provider CertEurope, declares that the demand for their eSignature solution increased by 200% between May and June 2020.¹¹⁰

The results from the OPC further underpin the increased use made of eID and trust services as a response to the COVID-19 pandemic. 59% of respondents have found the availability of the eID means or the electronic trust services (e.g. electronic signature) particularly useful during the lockdown measures introduced due to the COVID-19 crisis. A majority of respondents agreed that the eID and trust services should be extended as a result of the COVID-19 crisis¹¹¹.

Q9. To what extent do the solutions and standards address user needs?

Electronic identification

Need for support of major identify standards to facilitate user journeys

In the field of electronic identification, the eIDAS Regulation has put in place a common protocol based on an adaptation of the SAML protocol to exchange assertions between the different notified eID schemes and ensure a technical and semantic interoperability. The SAML message format and the attributes profiles have been adopted and maintained as part of the eIDAS eID profile.¹¹² The choice of this standard does not directly affect users, as identity providers remain free to use other types of protocols to manage their identity (e.g. OAuth2, OpenID). The eIDAS protocol is only used to exchange the identity information and authentication assertion between eIDAS nodes and across borders.

The choice of the SAML protocol was made at a time when most digital interaction took place via a desktop PC. Over the last years, mobile has become the preferred channel of digital interaction for most EU citizens. In 2018, 86% of persons aged 16 to 74, who used the internet over the past 3

¹⁰⁹ Legifrance, Décret n° 2020-395 du 3 avril 2020 autorisant l'acte notarié à distance pendant la période d'urgence sanitaire, see: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041781728/#:~:text=Copier%20le%20texte-.D%C3%A9cret%20n%C2%B0%202020%2D395%20du%203%20avril%202020%20autorisant.la%20p%C3%A9riode%20d'urgence%20sanitaire&text=Il%20d%C3%A9termine%20les%20conditions%20et.acte%20notari%C3%A9%20sur%20support%20%C3%A9lectronique.>

¹¹⁰ Oodrive, COVID-19 accelerates companies' use of electronic signatures, see: <https://www.oodrive.com/weareoodrive/group-news/press/covid-19-accelerates-companies-use-electronic-signatures/>

¹¹¹ Detailed results: Support to an extension of the eIDAS Regulation in general (64% of respondents), the eIDAS legal framework for cross-border eID in Europe (69% of respondents), the availability of eSignature (77% of respondents), eSeal (70% of respondents), eTimestamp (66% of respondents), ERDS (68% of respondents) and website authentication (54% of respondents).

¹¹² CEF Digital, eIDAS eID Profile, see: <https://ec.europa.eu/cefdigital/wiki/x/dATvB>

months, accessed the internet via a mobile or smartphone.¹¹³ With SAML the user authentication journey might be interrupted in case the citizens uses a mobile application although workarounds exist.¹¹⁴ Some stakeholders criticise the customisation of the SAML open standard to implement the principle of mutual recognition of eID schemes and suggest to support several major identity standards at the EU level, in line with the approach adopted for trust services.

Need for enhanced cryptographic requirements to avoid identity theft and privacy concerns

In terms of cryptographic requirements for the interoperability framework,¹¹⁵ the communication between the components of the eIDAS network and the citizen's browser is secured by the TLS protocol (Transport Layer Security). The current technical specification adopted on 27 September 2019 indicates that the eIDAS nodes must use at least TLS 1.2 released in 2008.¹¹⁶ Although this protocol is still considered as secure, some vulnerabilities have been discovered and concerns with regard to performance and privacy have been raised. A newer version of TLS (version 1.3) has been released in 2018.¹¹⁷ A delay in the adoption of version 1.3 may create risks for the protection of users against identity theft and guarantee the protection of their privacy and personal data.

User journey

The specificity of the eIDAS solutions means that different stakeholders are involved during the cross-border authentication journey. A group of Member States eIDAS experts have worked together over the past 3 years as part of a User Experience (UX) working group to further analyse the user journey.¹¹⁸ A series of pain points has been discovered and recommendations have been issued to Member States to improve the overall experience of the cross border authentication process. The key elements that have been pinpointed are the confusion that can be created for the users linked to the multiple redirections between the service providers, the eIDAS node interfaces and the identity providers. The lack of common visual identity and differences in user interface (UI) decrease the trust of users in the authenticity of the transaction process

Trust services

In the field of trust services, two implementing decisions have been adopted to provide:

- Specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies (Commission Implementing Decision (EU) 2015/1506 of 8 September 2015)¹¹⁹
- Standards for the security assessment of qualified signature and seal creation devices (Commission Implementing Decision (EU) 2016/650 of 25 April 2016)¹²⁰

¹¹³ Eurostat, EU survey on the usage of ICT in households and by individuals 2018, EU-27, see: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_usage

¹¹⁴ See: <https://www.mutuallyhuman.com/blog/choosing-an-sso-strategy-saml-vs-oauth2/>

¹¹⁵ CEF Digital, eIDAS eID Profile, see: <https://ec.europa.eu/cefdigital/wiki/x/dATvB>

¹¹⁶ Internet Engineering Task Force, The Transport Layer Security (TLS) Protocol Version 1.2, See: <https://tools.ietf.org/html/rfc5246>

¹¹⁷ Internet Engineering Task Force, The Transport Layer Security (TLS) Protocol Version 1.2, See: Internet Engineering Task Force, The Transport Layer Security (TLS) Protocol Version 1.3, See: <https://tools.ietf.org/html/rfc5246>

¹¹⁸ CEF eID, Final report on the user experience of the eIDAS-based eID, 31 July 2018 see: <https://ec.europa.eu/cefdigital/wiki/x/aZ4iAw>

¹¹⁹ 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, see: https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1506_en_txt.pdf

¹²⁰ COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No

According to industry, the implementing decision (EU) 2016/650 does no longer respond to user needs in view of its focus on smart card based solutions. Since the uptake of such solutions are low and remote server signing has become the norm, industry has called for an update to the implementing decision which is planned for 2021.

The lack of a legal recognition of such use cases has led to the application of alternative certification schemes at national level, leading to market fragmentation.

Meanwhile, two new CEN standards have been published by CEN TC224. ENISA recommends to update Commission Implementing Decision (EU) 2016/650 with the integration of the new standards. This recommendation is supported by several consulted stakeholders, notably EUROSMART,¹²¹ the trade association of the Digital Security Industry, as well as FESA, the Forum of European Supervisory Authorities for Trust Service Providers¹²² which call for a clarification of Annex II of the eIDAS Regulation on the requirements for QSCDs. Work has started with a view to a possible update of Commission Implementing Decision (EU) 2016/650 with the CEN Protection Profile for QSCD for Server Signing to reduce the current fragmentation of the market in this domain.

Q10. To what extent are there adaptation mechanisms in place to follow technological, scientific and social developments?

The eIDAS Regulation has been conceived technology neutral to accommodate the expected technological, scientific and social developments in this area. There have been however some trends or developments that required further guidance, cooperation or amendments to the legal framework. The evaluation revealed that, in general and despite technological changes and thanks to its technological neutrality, the basic design and implementation approach of the regulation still holds. Technological changes, such as blockchain and IOT, do not pose serious challenges and can be dealt with through amendments rather than overall “system change” or in implementation. However, the speed of implementation did not turn out to be high enough to roll out innovation in time.

Electronic identification

The eIDAS Regulation puts in place strong governance mechanisms to support its implementation. For eID, the eIDAS Cooperation Network has been created by Commission Decision (EU) 2015/296 and is composed of Member States experts meeting approximately three times a year to discuss opinions on new eID schemes and exchange information, experience and good practice in the field of electronic identity.

In addition, the implementation of the Regulation is supported by the eIDAS Expert group¹²³ which discusses the need for secondary legislation both for eID and trust services and also acts in comitology. A subgroup of the eIDAS Expert group focuses on electronic identity, it meets at least five times a year and maintains the eID technical specifications adopted by the eIDAS Cooperation Network.

Trust services

For trust services, the eIDAS Regulation relies on international standards defined by recognized standardization organisations such as ETSI, CEN, ISO, etc. These organisations are organised by

910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, see: https://ec.europa.eu/futurium/en/system/files/ged/celex_32016d0650_en_txt.pdf

¹²¹ EUROSMART, Answer to the European commission’s public consultation, October 2019, see: <https://www.eurosmart.com/on-the-application-of-eidas-regulation/>

¹²² FESA, Position Paper on the review of the eIDAS regulation, March 2020, see: http://www.fesa.eu/public-documents/FESA_Position_Paper_eIDAS_2020_Review.pdf

¹²³ <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3032>

expert working groups and aim at maintaining the standards along with the latest technological and societal development.

Supervisory bodies are exchanging best practices in the framework of the ENISA Article 19 Expert group and FESA, however these are informal groups where participation is voluntary and decisions non-binding. Several stakeholders¹²⁴ have called for formalising this cooperation similar to what has been foreseen under chapter II of the eIDAS Regulation with the creation of the eIDAS Cooperation Network.

The eIDAS expert group is one of the few official entities that tasked to follow the evolution of technical trends and to ensure that the eIDAS framework remains up to date.

Q11. To what extent has the eIDAS Regulation addressed relevant needs in specific sectors and what other areas should be covered?

Electronic identification

The notified eIDs under the eIDAS Regulation usually consist of “foundational identities”, meaning that they aim at providing citizens with an identity for diverse use cases. Notified eID under eIDAS include a minimum data set¹²⁵ which corresponds to a core set of information associated with a foundational ID system. The eIDAS technical specifications¹²⁶ foresee that additional attributes can be proposed by Member States to address sector-specific requirements. Although a number of Member States are interested in defining additional attributes, discussions are ongoing in the eIDAS eID technical subgroup since 2017 without that an agreement how to handle requests for sector-specific attributes has been found.

The increasing demand in the private sector that is obliged by sectoral legislation to identify citizens and business is a trend that is likely to continue with other fields, as more (and more valuable and more complex) transactions in the private are conducted online and companies move from providing products to providing services (software, mobility, infrastructure, utilities, etc), that require maintaining a long and ongoing relation with customers instead of “sell and forget” attitude. This coincides with the move of big platforms (GAFAMs) into the private identity market, posing the medium term risk of them dominating yet another area.

eHealth sector

In the domain of eHealth, a specific study was conducted to explore the use of eID in the eHealth domain.¹²⁷ More specifically, access to patient summaries and ePrescriptions in a cross-border context was explored. The study concluded that the eIDAS network could accommodate the exchange of sector-specific attributes such as a (pseudonymised) patient ID or the direct notification of an eHealth eID solution. In this context, the identification of health professionals is also required and associated to different levels of authorization to patient information. Again, it has been concluded that the eIDAS framework could in principle support this use cases.¹²⁸ The HEALTHeID project has piloted the reuse of the eIDAS nodes from four countries to perform

¹²⁴ See the governance section under effectiveness.

¹²⁵ The minimum data set includes: Family name, first name, birthdate and a national unique identifier as persistent as possible in time (typically a National ID number).

¹²⁶ eIDAS Technical Sub-group (2019), eIDAS SAML Attribute Profile v1.2. Available at <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile>

¹²⁷ DIGIT, The use of CEF eID in the CEF eHealth DSI, 2016, see: https://ec.europa.eu/cefdigital/wiki/download/attachments/37766100/DG%20DIGIT%20-%20The%20use%20of%20eID%20in%20eHealth%20-%20Final%20Report%20%20v3_0.pdf?version=1&modificationDate=1486488638015&api=v2

¹²⁸ eHealth Network, Recommendation paper on policies regarding eIDAS eID and Health Professional Registries, see: https://ec.europa.eu/health/sites/health/files/chealth/docs/ev_20180515_co11b_en.pdf

patient identification and authentication procedures in the current Cross Border eHealth Information Services (CBeHIS).¹²⁹

Yet, several concerns in the eHealth domain currently limits the reuse of eIDAS to offer simple and cross-border identification to patients and health professionals:

1. The current coverage of notified eID schemes is not sufficient in Europe and in many countries, there is a mismatch between the population that can access health services and those that can obtain an eID (e.g. children, asylum seekers, etc...)
2. The health domain requires a high level of assurance with regard to the patients and health professional's identity, effectively restricting the use to eID schemes with level of assurance 'high'.

Education sector

Europass Digital Credentials¹³⁰ provide an infrastructure for any educational organisation in Europe to issue user-held, digitally sealed credentials for its learners. The system uses eSeals to identify the issuing organisation as well as to secure the integrity of the documents issued.

A study was conducted in 2018 to understand the requirements of the education sector in terms of granting access to educational services, as well as to identify any technical or regulatory constraints.¹³¹ The study proposes to enrich the eIDAS minimum dataset with sector-specific attributes for cross-border student authentication. The CEF programme supports financially projects aiming at facilitating, simplifying and improving the quality of mobility of students across Europe. A specific EU student eCard support structure within the CEF programme has been created to demonstrate in practice the ability for academic and non-academic services to exchange student identity data.¹³² In parallel, the Horizon 2020 project Future Trust has also piloted¹³³ the possibility to combine academic ID and national ID in order to issue trustworthy certificates for creating an EU Student eCard.¹³⁴

Banking sector

The banking sector is subject to important regulatory requirements. An initial study on the use of on eID for digital on-boarding¹³⁵ explored how the eIDAS Regulation could allow financial institutions to better meet legal obligations in the fields of know-your-customer (KYC), Anti-Money Laundering, and strong authentication of parties (the Payment Services Directive 2). The study concluded that important attributes for natural persons (e.g. nationality, email, occupation) and legal persons (e.g. country of registration, email) were missing in the eID dataset.

In order to advance trusted electronic identification in the financial sector and remote Know-Your-Customer processes an expert group was created¹³⁶. The group focused on:

¹²⁹ HEALTHeID, eHN update on technical implementation and Member States participation in the HEALTHeID Transferathon, November 2019, see: https://www.spms.min-saude.pt/wp-content/uploads/2020/01/eHN_Nov_2019_HEALTHeID_Final.pdf

¹³⁰ <https://ec.europa.eu/futurium/en/europass/europass-digital-credentials-infrastructure>

¹³¹ DIGIT, Final report about Architectural Solution Document (eStudent), see: <https://ec.europa.eu/cefdigital/wiki/x/FZiuB>

¹³² CEF Programme 2019, see: https://ec.europa.eu/inea/sites/inea/files/cef_telecom_work_programme_2019.pdf

¹³³ eID.AS, FutureTrust releases eIDAS-Portal to kick-off "EU Student eCard" and demonstrators for eMandates, eInvoices and eApostilles, see: <https://www.eid.as/news/futuretrust-releases-eidas-portal-to-kick-off-eu-student-ecard-and-demonstrators-for-emandates-einvoices-and-eapostilles/>

¹³⁴ <https://ec.europa.eu/digital-single-market/en/eu-student-ecard>

¹³⁵ <https://publications.europa.eu/en/publication-detail/-/publication/8da08249-49cd-11e8-be1d-01aa75ed71a1>

¹³⁶ COMMISSION DECISION of 14.12.2017 setting up the Commission expert group on electronic identification and remote Know Your-Customer processes, See: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=36277&no=1>

- Establishing a mapping of existing remote on-boarding solutions in the banking sector and exploring issues related to eID and remote KYC processes;¹³⁷
- Suggest a framework for portable KYC/CDD solutions and a minimum set of needed attributes with the appropriate level of assurance (LoA) based on eID/eIDAS.¹³⁸

Travel documents and aviation sector

The aviation sector is required to control the identity of travellers and subject to hefty fines in case of non-compliance. A publication from the European Commission includes a review of the regulatory requirements imposed on airlines and the latest trends affecting the industry¹³⁹. Regarding support by eIDAS to different aviation use cases, the paper concludes that eIDAS solutions could be leveraged to tackle issues linked to incorrect data entry during the booking and onboarding phases. Yet, the current eIDAS minimum data set does not include all the necessary information for this purpose and sector-specific attributes would have to be defined, notably attributes covering passport and visa information.

In the travel document sector, the International Civil Aviation Organisation (ICAO) has developed and agreed on Digital Travel Credentials (DTC)¹⁴⁰, which should facilitate travel and border control through the digitalisation of the information in the electronic machine readable documents (eMRTD). One of the possible implementation options of the DTC in Europe could be linked to the eID function, using the same platform. Users would in this case not only use the eID for cross border services but they could also activate it as a substitute for the identification and authentication functions currently provided by physical travel documents.

Customs & Taxation sector

The European Commission has set up an identification and authentication system to allow traders and Economic Operators (EOs) to access the unified European Information System for customs, called UUM&DS (Uniform User Management and Digital Signatures Project) following adoption of Regulation (EC) No 766/2008. In 2019, it has been decided that UUM&DS identification and authentication could be performed via the eIDAS nodes and therefore reduce the costs of maintaining two systems with the same aim. In spring 2019, the UUM&DS team presented the required sector-specific attributes to the eIDAS eID technical subgroup. The integration is ongoing according to latest information

Trust services

Commission Delegated Regulation (EU) 2018/389 with regard to Regulatory Technical Standards (RTS) for strong customer authentication and common and secure open standards of communication in the context of the Payment Service Directive (EU) 2015/2366 defines how eIDAS solutions such as eSeals and/or website authentication can be used to identify third party providers when accessing Payment Service Providers' websites. The European Banking Authority

¹³⁷ https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf

¹³⁸ https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-december2019_en.pdf

¹³⁹ These include the need for increased accuracy driven by the adoption of the 2016/681 PNR directive of 27 April 2016 (<https://eur-lex.europa.eu/eli/dir/2016/681/oj>), requesting airlines to pass on passengers' PNR data to national authorities; the societal trend requiring better user experience during the booking and boarding experience for travellers and the emergence of blockchain solution aiming at creating verified data base of users to reduce the costs of future verification process. Source: CEF Digital, Study on opportunities and challenges of eID for Aviation, see: <https://ec.europa.eu/cefdigital/wiki/x/BYyuB>

¹⁴⁰ <https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Digital%20Travel%20Credential%20%28DTC%29.pdf>

(EBA) has also adopted an opinion on the use of eIDAS certificates under the abovementioned RTS and ETSI has issued standards to support meeting the regulatory requirements of PSD2.¹⁴¹

Q12. To what extent have alternative solutions been developed to address current needs, in parallel with the mechanisms and solutions foreseen by the eIDAS Regulation?

Electronic identification

In particular in banking and finance, alternative digital identity solutions have been developed in order to respond to regulatory requirements imposed on their commercial activity.

Some stakeholders consider identity data too sensitive to store centrally and suggest to consider decentralised systems for issuing trusted certificates based on distributed ledger technologies and self-sovereign identity solutions (SSI). The Commission has issued a discussion paper on how eIDAS solutions could support these technologies¹⁴². The conclusion is that the eIDAS Regulation can support the further development of such solutions either by linking the decentralised identity solution with a notified identity scheme under eIDAS, or with the use of digital electronic certificates (eSignature or eSeals) to support the issuance of verifiable claims.

Increasing use of mobile devices

The usage of mobile in Europe has sharply increased since the introduction of the eIDAS Regulation, both among users and digital identity schemes reusing the secure elements and sensors of mobile devices to offer their services. As a result, 90% of respondents in the OPC stated that the ability to use their eID on their mobile phone important for them.

Today, six out of the 14 countries that have notified an eID schemes have notified mobile solutions. A Commission report lists the different ways in which Member States support digital identity from mobile phones:

- *Making smartcard-based eID compatible with mobile devices:* Nine eID out of 18 smartcard based eID have enabled NFC communication technology which allows to read smartcards with a NFC equipped mobile phone¹⁴³.
- *Using mobile devices directly as an identification means:* SIMs are in principle technically identical to chips on smartcards and can therefore be used to host digital certificates for authentication as demonstrated by Estonia and Finland. Recent mobile phones also include secure elements isolated from the rest of the system for higher security which can also be used to store ID certificates. In this context, the concept of embedded SIM cards (eSIM) has been made available on Android phones since 2017.

Trust services

There is a need for improvement in certain trust services, in particular the provision of QWACs, which were introduced by the Regulation to enforce EU rules on a ‘right to know’ regarding the identity of websites. They offer traders and consumers a trusted and secure way of identifying the entity responsible for a specific website in a transparent way. Outside the browser environment, QWACs are used in the EU to secure payment services where full assurance on the identity of the

¹⁴¹ ETSI, Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366, see: https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.03.01_60/ts_119495v010301p.pdf

¹⁴² European Commission eIDAS supported self-sovereign identity, see: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

¹⁴³ Initially, access to the NFC function of Apple devices was restricted. In January 2019, the eIDAS Cooperation network called on the manufacturer to open access to its NFC interface to support secure mobile use of electronic identification means. In September 2019, Apple announced that its devices will be able to be used as readers for contactless eID smartcards.

entity behind a website is required by law. However, web browsers refuse to include QWACs in their root stores and to display them clearly, which makes these certificates unusable for traders and consumers. Although the Commission initiated a dialogue in 2018 to promote implementation of QWACs in the browser environment, web browsers continue to refuse supporting QWACs and have been unable to present alternatives with the same degree of legal assurance. Supporting a higher level of security, transparency and trustworthiness as offered by QWACs is not considered necessary by web-browsers and not foreseen by US legislation where most browsers are located. Web browsers are primarily concerned about ensuring the secure and trustworthy link to a domain and less about ensuring the identity of the entity behind the website with a high level of assurance as provided by QWACs.

Some stakeholders caution against the binding of QWACS to a Transport Layer Security (TLS) certificate as it is currently discussed within ETSI. Such binding would not be aligned with the principle of technological neutrality of the eIDAS Regulation and undermine interoperability and privacy for end users. TLS certificates are used to authenticate a server as part of a TLS connection while QWACs are used to guarantee the legal identity of a website owner. The nature and lifecycle of the legal entity of the organisation owning the website differs from the registration of a domain name. These alternative solutions to QWACs do not offer the same legal protection as they do not enable the consumer to trace a website back to the identity of the person or to the legal entity behind it. In addition, they do not assure that this person or legal entity is genuine and legitimate, which is important to prevent identity fraud. TSL certificates only inform about interaction with an identified entity. However, they cannot distinguish the identity of the actual owner of the site from the identity of an intermediary.

Q13. How does the eIDAS Regulation support the requirements for customer data portability and the emerging paradigm of full user control of personal data (as proposed by MyData or the Decentralised Identity Foundation)?

In terms of the data portability, the eIDAS Regulations in its current state does enable full data portability of identity attributes. However, the list of attributes included in the minimum data set for natural and legal persons as defined in the Annex of Commission Implementing Regulation (EU) 2015/1501¹⁴⁴ is too restrictive and does not enable a full deployment of an ecosystem. The possibility to adopt sector specific attributes is foreseen, but they are not covered by the level of assurance defined for the minimum data set which potentially decreases trust in such attributes.

Know your customer and Customer Due Diligence

The Recital 22 of the 5th Anti-Money Laundering Directive makes an explicit reference to the use of notified eID schemes to perform accurate identification and verification of natural and legal persons. Article 13 of the directive specifies that notified eID schemes under eIDAS are recognized as a valid solution to identify customers and obtain ID information about them. In the Annex III of the directive, specific dispositions recognise the possibility to use notified eID schemes to perform remote onboarding and verification of business relationships and transactions at distance.

However, several challenges are linked to this framework:

- There is currently no certification scheme to identify “trusted sources” and/or third parties to issue credentials, including KYC attributes;
- KYC requires attributes that reflect a current situation and are refreshed or updated under certain conditions;

¹⁴⁴ Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) 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, see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0001

Control of credentials by the users

In a survey of EU citizens, it was found that a large majority of respondents (63%) thought that it would be useful to own a secure single digital identity to access both public and private services and get control over the use of their data. The current Chapter II of the eIDAS Regulation does not enable this type of use cases, however an adaptation of the Chapter III on trust services to support the development of verifiable claims could.

Verifiable claims consist in a set of attributes about one person's identity (e.g. ID information), qualification (e.g. driving license, diploma), achievement (e.g. reached majority), quality (e.g. immunization against a disease). The W3W has been developing standards for expressing and exchanging "claims" verified by a third party as well as working on the definition of a verifiable credentials data model.¹⁴⁵

Several initiatives aiming at exchanging verifiable credentials are emerging:

- The European Blockchain Services Infrastructure (EBSI) has implemented a generic Self-Sovereign Identity (ESSIF) capability that will be integrated and interoperable with existing legal frameworks like eIDAS and GDPR;¹⁴⁶
- The European Commission has developed the Europass Digital Credentials and the Europass Learning Model that supports authentication services for any digital documents or representations of information on skills and qualifications as outlined in Article 4 (6) of the Europass Decision.¹⁴⁷ Europass operates a verifiable credential enterprise wallet with over 1.2 million users to accept degrees, diplomas, letters of recommendation, skill certificates and other documents representing professional or learning achievement. The Commission is working extensively with Member States and providing public information to software vendors to help them integrate secure digital credential recognition directly into credentialing, admission and recruiting infrastructures.
- The Covid-19 outbreak has fostered the creation of the COVID-19 Credentials Initiative (CCI). The community is composed of more than 300 individuals from over 100 organisations. The group is looking to deploy privacy-preserving verifiable credential projects in order to mitigate the spread of COVID-19 and strengthen societies and economies.¹⁴⁸ They have notably developed a data model supporting the creation of immunization passport that could help citizens to prove their immunization status either by testing or vaccination.
- The creation of eVisa or ePassport.¹⁴⁹

Reuse of identity verification procedures

Citizens and business are asked to prove their identity more and more in their daily activities. However, there is currently no possibility to rely on pre-existing identity verification procedures to comply with e.g. KYC requirements. As a consequence, there is a multiplication of identity and KYC verification procedures (remotely or in persons) in Europe, leading to unnecessary costs both for customers and companies subject to regulatory requirements in terms of identity verifications.

¹⁴⁵ Only an identity verified by a trusted entity can be recognized to fulfil regulatory requirements (under e.g. AML, PSD2, etc...) or for generating trust with relying parties. The creation of specific trust services to guarantee that the verifying party is a trusted entity could be supported by the creation of a specific trust service providers. - W3C, Verifiable Credentials Use cases, 24 September 2019, see: <https://www.w3.org/TR/vc-use-cases/>

¹⁴⁶ https://medium.com/@SSI_Ambassador/essif-the-european-self-sovereign-identity-framework-4572f6875e12

¹⁴⁷ Europass, What are digital credentials, see: <https://europa.eu/europass/en/what-are-digital-credentials>

¹⁴⁸ <https://www.covidecreds.com/#Workstreams>

¹⁴⁹ WEF, The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel, see: http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf

In order to be fully aligned with GDPR requirements, these types of credentials could be further computed in zero-knowledge claims, allowing the holder of such credentials to only disclose minimal information to relying parties: e.g. a proof of majority rather than the sharing of the person's actual date of birth.

Q14. How well adapted is the intervention to subsequent technological or scientific advances? What are the opportunities for expanding the number of trust services currently covered by the Regulation (by e.g. blockchain, eArchiving, IoT) and for extending eID services to the private sector?

The majority of stakeholders consulted agreed that the eIDAS Regulation should be expanded to include other trust services (e.g. eArchiving) and that the number of trust services covered by the Regulation could be expanded in its current form.

Blockchain

Use cases linked to the issuance of electronic identity in a decentralized fashion have multiplied over the last years. Although such solutions have not yet reached a critical mass like “traditional” electronic identity solutions, it is important to ensure that the eIDAS Regulation will be able to address these emerging use cases. In the case of the use of blockchain or distributed ledger technology, the notion of single identity provider is questioned. In the case of a distributed system, attributes may be endorsed by a variety of different stakeholders. It is therefore important that the attributes provided by this parties can reply to a set of defined criteria.

A study has been contracted by the European Commission to evaluate how eIDAS can legally support digital identity and trustworthy Distributed Ledger Technology – based transactions in the Digital Single Market.¹⁵⁰ The study provides useful scenarios on how self-sovereign identity use cases could be supported by the eIDAS Regulation.

- On the very-short term and without any modification to the eIDAS Regulation, notified eIDAS eID means and qualified certificates could be used to issue verifiable credentials (cf. prior section). An eIDAS “Bridge” has been developed to increase the verifiable credentials’ legal value and cross-border recognition.¹⁵¹ The current eIDAS nodes could be upgraded to start issuing SAML assertions based on verifiable credentials.
- On the short-term and within the framework of the current eIDAS Regulation (i.e. by modifying existing implementing acts), verifiable IDs could be recognized as notified eIDAS schemes and qualified certificates could be issued based on a specific decentralised identity method and verifiable credentials.
- In the mid- to long-term, the eIDAS Regulation could be amended to extend the eIDAS notification mechanism to verifiable claims, new trust services could be created to regulate the issuance of verifiable attestations, regulate identity hubs and ensure key management and operation of DLT nodes.

eArchiving

The preservation of electronic signature is a market under development. The eIDAS Regulation does require the archiving the signature of electronic document. However, the eIDAS Regulation

¹⁵⁰ European Commission, SSI eIDAS Legal Report, How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market, see: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

¹⁵¹ JoinUp, About SSI eIDAS bridge, see: <https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about>

does not specify requirements and standards to use. Several stakeholders have mentioned that eArchiving should be added to the list of trust services.¹⁵²

Some Member States, like Luxembourg, have defined national rules and seven public and private organisations currently offer such services accordingly.

The current ‘Long-Term Archival’ standards for digital signatures and seals provide for a ‘resigning’ mechanism whereby a signed document is resigned every few years to maintain its validity. Any error with resigning, or a late resigning of a document, will break the signature chain and render the document invalid. This solution means that only specialised ‘archival servers’ can be used to store documents for a long period. Use cases such as allowing a user to store documents on their own device become impossible.

Internet of Things

One of the latest trends in the field of digital identity is the need to provide an identity to things in light of the growing importance of the Internet of Things (IoT). The number of connected devices installed globally could more than triple from 23 billion in 2018 to over 75 billion in 2025.¹⁵³ Along with this rapid increase comes a critical risk of identity theft and manipulation, which leads to the **need for effective identity and security solutions for IoT**. Security incidents arise because traditional identity and access management systems have difficulties to adapt to the proliferation of connected devices as they focus exclusively on people and are not built for the IoT.¹⁵⁴ Organisations as well as governments face significant financial, reputational and legal consequences as a result of cyberattacks and data leaks.¹⁵⁵ Consequently, key players in the field of IoT are pushing for an evolution of the identity market that meets their needs.

Thus, global identity management can no longer only focus on users but needs to take into account all entities in the transactional ecosystem. It was previously enough to manage the identity of a person connected to an application, service or device, but now the relationships between different devices, applications and services need to be managed as well. This is even truer as AI applications become a reality and the use of automated devices progress. Within an **ecosystem of the Identity of Things (IDoT)**, where all entities have the same interaction framework, digital identity platforms are evolving to be able to establish secure and trusted relationships across the full spectrum of the IoT ecosystem, using a concept of continuous authentication and being context-aware.¹⁵⁶

The current eIDAS interoperability framework only includes a dataset for natural and legal persons. Consulted stakeholders propose to explore how similar datasets could be developed to support IoT use cases.

¹⁵² One stakeholder also mentioned the possibility to create a separated trust service linked to the digitization of documents, consisting in providing minimum requirements and standards for the action of converting paper documents into electronic documents before archiving.

¹⁵³ NewGenApps (2018), 13 IoT Statistics Defining the Future of Internet of Things, <https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data>

¹⁵⁴ Gartner (2015), Gartner Says Managing Identities and Access Will Be Critical to the Success of the Internet of Things, <https://www.gartner.com/newsroom/id/2985717>

¹⁵⁵ SecureID (2016), How identity can fix the IoT, <https://www.secureidnews.com/news-item/how-identity-can-fix-the-iot/#>

¹⁵⁶ European Commission (2018), Trends in electronic identification - An overview, https://ec.europa.eu/cefdigital/wiki/download/attachments/78549570/Trends%20report%20on%20electronic%20identification_for%20publication_v.1.1.pdf?version=1&modificationDate=1551198712785&api=v2

5.4 Coherence

This section presents the main findings from the legal desk research and preliminary stakeholder consultation aiming to inform the evaluation with questions on the internal and external coherence of the provisions of the Regulation.

Q15. Are there issues of internal coherence (i.e. between parts of the eIDAS Regulation and implementing acts)?

The following issues with clarity or coherence have been identified through an article-by-article review of the eIDAS Regulation. Some of the obstacles identified below that would require further clarifications in the definitions would still not have major impact on the more successful implementation of the Regulation as the pertinent shortcomings related to the scope and the design of the framework would remain due to the dependencies on the sectoral or national legislation and administrative practices.

Another identified obstacle related to the shortcomings of the notification procedure and the assurance levels framework would need to be addressed in the revision of the Regulation in addition to the attempts to clarify them throughout discussions with Member States representatives on the update of the existing guidelines to date.

The difference in the liability regimes between the notified eIDs and the trust services framework is mirrored by the different regulatory regimes – the notification process is based on a mechanism of building trust between the Member States, whereas the trust services framework follows more the market based approach.

Definitions – Article 3

Certain definitions set out in Article 3 could benefit from clarification, reformulation or updating. In particular, the following examples have been noted:

- Article 3(1) currently defines authentication as “an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed”. Commission Implementing Regulation (EU) 2015/1501 provides a minimum set of identification data for a natural person, a legal person or for a natural person representing a legal person. However, it may be appropriate going forward to adapt eIDAS for the identification of a natural person *representing* a natural person (or even a legal person, not represented by a natural person, depending on the development of AI in the context of company law). This would not necessarily require an amendment of Article 3(1), but could be addressed by amending other aspects of eIDAS, such as Regulation (EU) 2015/1501;
- As per Article 3(12), a qualified electronic signature is an advanced electronic signature that is created by a qualified electronic signature creation device (see requirements in Annex II of the eIDAS), and which is based on a qualified certificate for electronic signatures (see requirements in Annex I). However, this definition does not include any reference to timestamping. This may be considered as a loophole as it opens up the possibility for a qualified electronic signature to be “self-dated”; thus no formal verification of the date of signing could be undertaken. Furthermore, some stakeholders argued that the formulation of Annex II in its current version is too permissive as it permits any qualified trust service provider to generate or manage electronic signature creation data on behalf of the signatory. This does not guarantee the highest level of protection to the holder of the qualified certificate.
- Article 3(16) the words “and” and “or” are deployed several times, so that the exact meaning is ambiguous. This is a simple drafting issue, and could be resolved by more appropriate syntax.

Provisions on eID

According to an assessment of the eID provisions, certain provisions show a lack of precision which may lead to inconsistencies in the application of electronic identification schemes. Additionally, certain provisions may constitute barriers to the use of electronic identification schemes by the private sector:

Conditions for notification – Article 7

Article 7 sets out certain pre-conditions for notification. From the perspective of a provider of a non-notified eID wishing to be notified, Article 7(b) may act as an obstacle. If a Member State has already notified a scheme, it may be difficult for a new eID provider to have its scheme recognised by a public authority for access to a public service. In turn, this may act as an obstacle to having the scheme notified.¹⁵⁷

Notification, peer review system and assurance levels

Assurance levels are a key component of the eIDAS interoperability framework. Article 8 provides for 3 such levels, while Commission Implementing Regulation (EU) 2015/1502 defines the minimum technical specifications and procedures in order to ensure a common understanding in the context of the interoperability framework. As required by Article 8(3), these technical specifications and procedures take into account relevant international standards (e.g. ISO/IEC 29115) and build on these, while taking into account the specific context of eIDAS. Implementing Regulation (EU) 2015/1502 notes that it is designed to be outcome based. This has the advantage of retaining flexibility and technical neutrality.

A number of issues have been noted in relation to assurance levels. Firstly, the system of mutual recognition envisages the recognition by a public sector body of an eID for cross-border authentication where the assurance level of that eID is equal to or greater than the assurance level which that public body requires to access its services. In a cross-border context, this could give rise to difficulties for a citizen of Member State A, living in Member State B and working in Member State C. He may have obtained an eID with an assurance level substantial in Member State A, and find that it is sufficient for his registration with the authorities in Member State B, but that it is not accepted by the tax authorities when attempting to file his tax return in Member State C. It is an issue which is likely to persist so long as there are different levels of assurance and the definition of the assurance level required is determined by the specific public sector body. eIDAS provides for different levels of assurance, but national rules are binary; one either identifies or one does not.¹⁵⁸ One stakeholder suggested that the solution may be to have a single assurance level, while another noted that the trend should be towards high, particularly if eID is to be used in sectors such as healthcare. In addition, there is incoherence between Chapter II (eID) which sets three-tiered assurance levels and Chapter III (trust services) which includes only qualified and non-qualified trust services.

Another issue with the current assurance levels is that they do not seem to have ensured the level of common understanding which they were intended to as the understanding of what is high or substantial differs among Member States.

¹⁵⁷ 67.61% of the respondents to the OPC either agreed or strongly agreed with the statement ‘The scope of the eIDAS Regulation should be extended to provide a level playing field for the private economic actors operating in the field of electronic identification.’ This can be contrasted with views regarding a level playing field for eSignature, in respect of which only 39.31% agreed or strongly agreed with the statement ‘The eIDAS regulatory framework creates a level playing field for electronic signature in Europe.’

¹⁵⁸ This problem is not entirely due to the eIDAS assurance framework but also the lack of a harmonised approach being taken by Member States in defining the levels of assurance for respective public services.

It has been suggested that the current assurance levels are not necessarily relevant for all entities in the private sector, who may be more interested in a risk-based approach and may have different priorities. For example, much of processes in place in the financial services sector for AML purposes are centred on a risk-based assessment. Entities in the financial services sector may appreciate being able to distinguish between an eID in the upper reaches of the substantial level and those on the lower reaches, as part of their risk assessments.

Liability as per Articles 11 and 13

In the impact assessment accompanying the proposal for eIDAS, one of the key issues noted was the need for clear liability for eID.¹⁵⁹ In the context of cross-border transactions, Article 11 seeks to address this. It sets out the division of liability between the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure. As for the latter, Article 11 (3) states that the party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication. However, the Regulation is silent on the way the “correctness” of the operation of the authentication should be evaluated.¹⁶⁰ This may be an important consideration given that Article 11 provides for a division of liability between the Member State (in respect of the obligation to ensure availability of authentication) and the party operating the authentication procedure (for failure to ensure correct operation of the authentication).

The division of liability may have considerable consequences. Different actors involved (private and public) could make each other responsible as it may be difficult to pinpoint the problem. In fact, it could be questioned whether Member States would take responsibility for parties other than the State itself to provide online identification and authentication services. However, Recital 13 of eIDAS states that “Member States should remain free to use or introduce means, for electronic identification purposes, for accessing online services. They should also be able to decide whether to involve the private sector in the provision of these means.”¹⁶¹ However, certain Member States rely on the private sector for the provision of eID means. Furthermore, eIDAS is silent on the possibility of the Member State including a clause in a contract with a private company, whereby the latter would indemnify the former in relation to authentication that may be outsourced to that company.

Furthermore, it may be that the possible exposure to liability might represent a disincentive for Member States to notify eID schemes¹⁶².

There is a clear difference between Article 11 (providing for liability in the context of eIDs) and Article 13 (in relation to trust services), in that the latter provides for the possibility of the trust service provider limiting liability provided they duly inform their customers in advance of such limitations and where those limitations are recognisable to third parties. Such limitation of liability is not provided for in Article 11. One issue which was raised during the consultation was the fact the risk of the eIDAS node being subverted. Regardless of the level of security of the national eID

¹⁵⁹ COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, p.10.

¹⁶⁰ Didier Gobert, „Le règlement européen du 23 juillet 2014 sur l’identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*

¹⁶¹ Colette Cuijpers, Jessica Schroers, “eIDAS as a guideline for the development of a pan European eID framework in FutureID, available at https://pdfs.semanticscholar.org/d45f/27687596bc1b04d571023de1bed287e9d0be.pdf?_ga=2.254795336.115807749.1575904709-297406062.1575904709 (last accessed on 10.12.2019).

¹⁶² Niko Tsakalakis et al., “Identity Assurance in the UK: technical implementation and legal implications under Eidas”, *Journal of Web Science*, Vol. 3: No. 3, pp 32-46.

system, the subversion of the node can lead to problems for users of that national ID in a cross-border context. This could expose the Member State in question to significant liability despite not being responsible. Article 11 could clarify this by clarifying the division of liability between the notifying Member State and the node operator.

Similarly, while Article 13 provides explicitly for the shifting of the burden of proof based on whether or not the trust service provider is qualified, no such explicit provision is set out in Article 11. Recital 18 makes it clear that national rules on the burden of proof are not affected. Another option might have been to treat notified eIDs in a similar manner to qualified trust services, explicitly shifting the burden of proof to the Member State, party issuing the eID means or the party operating the authentication procedure, in respect of Articles 11(1), 11(2) and 11(3) respectively. The advantage of such an approach would be to ensure consistency across Member States in relation to the rules on the burden of proof. However, a presumption of negligence or intention could have the impact of making Member States less likely to notify.

Finally, the issue of joint and several liability for controllers under Article 82 GDPR has been raised as adding to the complexity of the liability division, in the event that more than one party are deemed to be controllers in relation to personal data (e.g. in the event that the eID scheme is operated by a public and a private entity).¹⁶³

Lack of legal equivalence for eIDs / Article 14 for trust services

Legal equivalence determines whether eID services offered in third countries offer an equivalent level of protection to those in the EU. Hence, legal equivalence is conceived as a pre-condition for attaching specific legal effects to third countries' eIDs. However, legal equivalence is only defined in relation to trust services and not eIDs. Beyond the issue of not being able to qualify for mutual recognition (via notification), there is the practical issue of determining the level of assurance of the third country eID.

Article 14 covers trust services, but the threshold of being recognised under an agreement concluded between the EU and a third country or international organisation seems to set a high threshold for trust service providers. Nor does eIDAS clarify the steps in relation to reaching such an agreement. This can be contrasted with the approach in the GDPR, where Article 45 sets out detailed considerations regarding the process and criteria for arriving at adequacy decisions for transfers of personal data to third countries. While the target being assessed as well as the kind of outcome (unilateral decision by the Commission vs. international agreement) are different, Article 45 GDPR may provide inspiration for a process for recognition of trust services originating from third countries.

Provisions on trust services

Supervisory body and conformity assessment bodies as per Articles 17 and 20

Conformity assessment bodies (CAB) have no explicit liability under eIDAS resulting in practices such as QTSPs being audited twice by the CAB and by the Supervisory Body, the latter, not always trusting the Conformity Assessment Report. Lack of harmonisation with respect to the reporting requirements also leads to quality.¹⁶⁴ Hence, as per Article 20(4), there should be a more standardised procedure adopted via implementing acts in relation to the accreditation of CABs and in relation to auditing rules under which CABs carry out their conformity assessment (i.e.

¹⁶³ *Id.*, p.8.

¹⁶⁴ Several stakeholders noted that there is a huge variability in quality of CAB reports which could be linked to the person carrying out the assessment, but also linked to the trust service in question, while more than 40% trust service providers which responded to the stakeholder survey either disagreed or strongly disagreed with the assertion that the rules and procedures for verifying qualified status were consistent across the Member States, while more respondents to the survey questionnaire targeting supervisory bodies, conformity assessment bodies and national accreditation bodies disagreed than agreed that conformity assessment reports are of consistent and adequate quality.

establishment of a comprehensive list of requirements that CABs must use when carrying out the conformity assessment).¹⁶⁵ Some stakeholders proposed a standard for accreditation of auditors. These auditors could then apply best practice, which would be based on “recognised sources”. Such recognised sources could be standards developed by entities such as ETSI or ISO. The idea would be to ensure a certain level of quality of audits, while retaining a degree of flexibility. It should be noted that ENISA has made recommendations regarding standardisation for auditors.¹⁶⁶

Furthermore, there is a need to clarify the liability scheme for CAB’s activities once a standardised procedure has been adopted: if a CAB is liable towards the Supervisory Body on the audited perimeter, the Supervisory Body should trust the conformity assessment report which would thus play the actual role of ex-post auditing authority over QTSPs.¹⁶⁷ This would reduce costs and help speeding up the processes as called upon by stakeholders consulted.

Security requirements applicable to trust service providers as per Article 19

As per Article 19, QTSP and non-QTSPs shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Several stakeholders consulted suggested that eIDAS should set out basic security requirements trust service providers should follow (e.g. EN 319 403 and EN 319 411-1).

Body responsible for establishing, maintaining and publishing national trusted lists as referred to in Articles 21 & 22

As per Article 21 (2), when the supervisory body grants qualified status to the trust service provider and the trust services it provides, it shall inform the body responsible for establishing, maintaining and publishing national trusted lists not later than three months after notification. However, the Regulation makes no mention of any timeframe to be complied with by this body in the update of its lists.¹⁶⁸ Neither does Commission implementing decision 2015/1505 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5).¹⁶⁹ However, as specified in 21 (3), qualified trust service providers can only begin to provide the qualified trust services once the qualified status has been indicated in the trusted lists managed by this body. It should be noted that this was not raised during stakeholder consultation as being an issue in practice.

Requirements for qualified trust service providers as per Article 24

Certain requirements of Article 24 have been noted as potentially generating inconsistencies in interpretation. For example, it is questionable whether the requirement of “physical presence” set out in Article 24(1)(b) is necessary given that identity verification is an integral part of the assurance level assessment. It has been suggested that this may not be consistent with the aim expressed in recital 16 of “ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for qualified certificates”. Indeed, some stakeholders note that certain remote identification means are more trustworthy than physical presence (e.g. biometric verification).

Several stakeholders consulted noted that the reference in Article 24(1)(d) to the use of “other identification methods recognised at national level” is inappropriate as the implementation of this

¹⁶⁵ In a survey of supervisory bodies, conformity assessment bodies and accreditation bodies, a large majority of respondents were of the view that further implementing acts were required. A majority of respondents to the survey targeting national authorities and eIDAS node operators were also of this view, as were qualified trust service providers.

¹⁶⁶ ENISA, Towards global acceptance of eIDAS audits, v1.1, May 2019.

¹⁶⁷ E.g. InfoCert: eIDAS Review InfoCert Group Contribution to the revision process of the eIDAS Regulation (2019), p.5.

¹⁶⁸ Didier Gobert, „Le règlement européen du 23 juillet 2014 sur l’identification électronique et les services de confiance (eIDAS) : analyse approfondie », *op.cit.*

¹⁶⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1505&from=EN> (last accessed on 10.12.2019).

notion diverges from Member State to Member State. Stakeholders called for a common understanding among Member States of this notion. This could be achieved by the issuance of further guidance as regards the verification by TSP of the specific attributes of the person to whom the qualified certificate is issued.

The requirements for qualified trust service providers would be more consistent across the EU if these requirements were further harmonised. For example, either physical presence is required in all cases or it is not, and if ‘other identification means’ can be relied on, these should be the same across all Member States. Going further, should it be explicitly clarified that physical presence is not required, the rules for remote identification would need to be introduced in order to guard against divergences. This would mean that the verification required by Article 24(1) would be more harmonised across all Member States.

Mutual recognition of electronic signatures as per Article 25 (3)

As per Article 25 (2), a qualified electronic signature shall have the equivalent legal effect of a handwritten signature. However, eIDAS does not harmonise the legal effects of handwritten signatures in the sense that the equivalent legal effect of a handwritten signature cannot be afforded to other types of electronic signatures. Today, the legal effects may be defined under national law leading to discrepancies among Member States. Consequently, the principle of mutual recognition of electronic signatures between Member States as laid down by Article 25 (3) may be restricted.¹⁷⁰ For example, some Member States may recognise electronic signatures (which are not qualified) as having the equivalent effect of handwritten signatures. Or national contract law might dictate that if the intention of the parties is for the electronic signature to have such effect, it should be held to have such effect.¹⁷¹

Qualified preservation service for qualified electronic signatures as per Article 34

The Regulation provides for a qualified preservation service for qualified electronic signatures. Whereas the trustworthiness of the qualified electronic signature is guaranteed beyond the technological validity period, the Regulation does not harmonise rules relating to a general electronic archiving service.¹⁷² Some stakeholders favour the introduction of a trust service for electronic archiving of documents which guarantees their readability through the adoption of standards ensuring that all the tools allowing access to the documents are maintained by QTSPs. Individual Member States already adopted laws providing a legal framework for electronic archiving. For instance, the Belgian legislator established a framework for electronic archiving aiming at covering all stages of the electronic process from the conclusion of the act, until the archiving of the latter.¹⁷³ As per Article 2 of that Law, electronic archiving is a trust service as per Article 3(16) of the eIDAS which consists in the conservation of electronic data or the digitisation of paper documents, and which is provided by a trusted service provider as per Article 3(19) of the eIDAS, or which is operated for its own account by a public sector body or a natural or legal person. Furthermore, the Belgian law distinguishes between non-qualified and qualified electronic archiving. However, only the latter benefits from a presumption of integrity relating to the content

¹⁷⁰ Didier Gobert, «Le règlement européen du 23 juillet 2014 sur l’identification électronique et les services de confiance (eIDAS) : analyse approfondie», *op.cit.*

¹⁷¹ Irene Kull, Laura Kask, «Electronic signature under the eIDAS Regulation in domestic and cross-border communication: Estonian example», *op. cit.*, p.28.

¹⁷² Didier Gobert, «Le règlement européen du 23 juillet 2014 sur l’identification électronique et les services de confiance (eIDAS) : analyse approfondie», *op.cit.*

¹⁷³ Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l’identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

of the documents stored.¹⁷⁴ Similarly, Luxembourg¹⁷⁵ and France¹⁷⁶ have adopted a legislation covering electronic archiving.

Electronic registered delivery service as per Articles 43 and 44

Contrary to other trust services, Article 43 does not mention any mutual recognition for electronic registered delivery services. Some stakeholders consulted pointed out that the wording in relation of the requirements of identification of sender and receiver stated in Article 44 could be specified. In fact, the current formulation refers solely to the “identification”, and seems depicting a situation where each time a message is sent or received, an identification process is required in compliance with Article 24 – this requirement would “inevitably create an incoherent process, with a poor user experience mirroring its wide adoption.”¹⁷⁷ Hence, these stakeholders suggested to specify that the requirements of identification of senders and receivers could be practically met with the identification at the creation of the delivery account and the authentication each time a message is sent and read.

Qualified website authentication certificates (QWAC) as per Article 45

As per Recital 67, website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity behind the website. This leads to the building of trust and confidence in conducting business online. In order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, minimal security and liability obligations for the providers and their services through qualified certificates for website authentication are laid down in Article 45. Whereas Article 45 provides that qualified certificates for website authentication shall meet the requirements laid down in Annex IV, it does not envisage any legal effects relating to this service. Thus, judges at national level shall determine these legal effects which may lead to discrepancies of legal effects among Member States.

Furthermore, stakeholders suggested that eIDAS should lay down a legal responsibility on web browsers and make them reliable for trustworthiness of websites. Currently, the conditions of issuance of website certificates depend on the commercial practices of producers of mainstream web browsers, thus they have no formal obligation to use QWACs. Some stakeholders noted that there is currently a lack of recognition of W3C and world-class internet browsers to integrate the use of QWACs – this deters users and organisations from investing them. However, consulted stakeholders noted that the level of guarantee provided by the web browsers is unknown to the user and most web browsers use very low levels of certification (e.g. domain validate certificate as opposed to an extended validation certificate, i.e. there is no identification of the natural or legal person linked to the website). On the other hand, web browsers access a lot of information from users. Hence, stakeholders argued that for special services where web browsers gain access to data from EU users, there should be even an obligation to use QWACs and to comply with European standards (e.g. public institutions at national and European level should be required to protect their websites with QWACs). Finally, web browsers should be required to publicly display QWACs. Further explanations have been provided in the previous sub-section - Relevance Q 12.

¹⁷⁴ Ibid.

¹⁷⁵ Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification: 1. de l'article 1334 du Code civil; 2. de l'article 16 du Code de commerce; 3. de la loi modifiée du 5 avril 1993 relative au secteur financier, Mémorial A n°150.

¹⁷⁶ Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°0035 du 11 février 2016 texte n° 26 ; Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283 du 6 décembre 2016 texte n° 61.

¹⁷⁷ E.g. InfoCert: eIDAS Review InfoCert Group Contribution to the revision process of the eIDAS Regulation (2019), p.6.

Q16. Are there coherence issues with relevant Member States' rules and regulations?¹⁷⁸

In May 2019, 17 out of 28 Member States had adopted implementation legislation with respect to eIDAS.¹⁷⁹ Whereas certain national requirements may exceed requirements of eIDAS (“goldplating”)¹⁸⁰, this assessment focuses on potential issues of incoherence between national provisions and the eIDAS Regulation. Incoherence may arise due to several factors:

1) Provisions which allow for diverging implementation by Member States:

A survey from December 2017 mentioned the lack of secondary legislation¹⁸¹ for the eIDAS Regulation and the lack of a clear road map for the development of eIDAS and trust services, which keeps on replicating harmonization gaps, as barriers for the development of the Trust Service market.¹⁸² The survey identified different interpretations of eIDAS requirements and / or definitions of trust services in Member States and the lack of harmonisation of practices by Supervisory bodies, and Conformity assessment bodies. The following examples were mentioned:

- eIDAS does not provide a definition of a unique identifier which leads to different practices, issues of identity matching and difficulties in data reconciliation.¹⁸³ A specific survey with the eIDAS Cooperation Network and eID Technical Subgroup representatives showed that one of the main blockers and issues identified by the Member States with respect to limited connections to the eIDAS infrastructure is the match to the national identifier. Extending the minimum data set and further harmonisation of rules on the unique identifier would address a number of secondary obstacles linked to the limited implementation of the current eID part of the Regulation.
- The designation of a supervisory body is left (as per Article 17 eIDAS) to Member States. However, national supervisory bodies may use different procedures to verify if requirements are met. The adoption of implementing acts (Article 21(4) laying down guidance on formats and procedures for Supervisory bodies may lead to a more homogenous verification of requirements and may also provide for a solid basis in case legal actions to be taken against a trust service provider that is not respecting those requirements. The need for more harmonised national qualification procedures between Member States has been pointed out by several stakeholders consulted. In fact, there are currently divergent approaches adopted by national supervisory bodies: whereas some

¹⁷⁸ Which corrective actions can be advised, e.g. adoption of secondary legislation, more guidance from the Commission and/or ENISA, including extending its role, tighter cooperation between Supervisory Bodies, more regular market analysis?

¹⁷⁹ https://ec.europa.eu/futurium/en/system/files/ged/compilation_ms_information_07052019.pdf (last accessed on 16.12.2019).

¹⁸⁰ For example: In Belgium, Article 1322 of the Civil Code adds a further condition to an electronic signature: the data in electronic form shall maintain the integrity of the content of the act - whereas under the eIDAS, an electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Fanny Hiéronimus, “Enjeux juridiques et impacts de la Blockchain pour le notariat et le secteur bancaire belge” - un travail écrit, 2017-2018, available at : <https://matheo.uliege.be/bitstream/2268.2/4867/4/TFE-FannyHIERONIMUS-DroitGestion-2017-2018.pdf> (last accessed on 17.12.2019).

¹⁸¹ It should be noted that several implementing acts have been introduced. However, there are still Articles in the eIDAS Regulation providing possibility for adopting additional implementing acts, which have not (yet) been enacted.

¹⁸² ENISA, “eIDAS : overview on the implementation and uptake of trust services, one year after the switch over”; December 2017.

¹⁸³ For example, in DE, the pseudonym created by the eID card was assigned as unique identifier. The legal implications of this decision have not yet been challenged in a court. It should be noted that the German Constitutional Court ruled in 1983 that the creation of any kind of unique identifier is forbidden. Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983, BVerfGE 65, 1, 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden“ <https://eprints.soton.ac.uk/413943/1/WebSciJournal.pdf> (last accessed on 9.12.2019).

Member States follow the requirements laid down by eIDAS, other Member States go beyond those requirements which creates risks of a race to the bottom.¹⁸⁴

- Article 24 sets out the requirements for qualified trust service providers. Article 24(1)(d) provides for the use of verification methods “recognised at national level” which provide equivalent assurance in terms of reliability to physical presence. This allows for divergent approaches among Member States as mentioned above. In practice, identity-proofing methods are defined in different ways at national level, some trust service providers face market-entry barriers. For example, remote identification using video identification is allowed in some Member States and not in others. This creates an uneven playing field benefitting trust services providers established in those Member States where the use of video identification is allowed.

2) National provisions and regulatory practices contradicting eIDAS:

The survey on trust services from December 2017 noted that “national level trust services non-conformant with eIDAS Regulation create uncertainty and confusion, hindering the uptake of the Trust Services Market”.¹⁸⁵ In the stakeholder survey conducted during the current evaluation, more than half of the respondents to the trust service providers survey agreed that there is legislation at national level which frustrates the goals of eIDAS and 40% of respondents to the OPC were of the view that legal obstacles (such as the requirement for face-to-face interaction under national law) were a limiting factor for the cross-border use of eIDs.¹⁸⁶ Some Member States, for example, demand specific technical requirements and specific data in certificates in order to access public services or public tenders.¹⁸⁷ The obstacles related to the incorrect implementation falling within the scope of the eIDAS framework at national level are monitored and addressed as part of the enforcement.

3) National provisions which may not take full advantage of the possibilities offered by eIDAS:

¹⁸⁴ For example, in Germany, national supervisory bodies must follow strict requirements going even beyond the ones laid down in the eIDAS in relation to the verification of the qualification of trust service providers. However, qualified status granted by a supervisory body following less strict requirements has legal effects in all EU countries as long as they comply with the requirements laid down in the eIDAS - i.e. EU Member States having implemented stricter requirements need to recognise those qualified trust services issued by national supervisory bodies following less strict requirements. - Steffen Schwalm, Theresa Vogt, “Die-Bedeutung der eidas Verordnung für Behörden-Chancen und Herausforderungen im e-government“ available at <https://docplayer.org/67398178-Die-bedeutung-der-eidas-verordnung-fuer-behoerden-chancen-und-herausforderungen-im-e-government-steffen-schwalm-theresa-vogt.html> (last accessed on 16.12.2019).

InfoCert: eIDAS Review InfoCert Group Contribution to the revision process of the eIDAS Regulation (2019), p.5.

¹⁸⁵ ENISA, “eIDAS: overview on the implementation and uptake of trust services, one year after the switch over”; December 2017.

¹⁸⁶ Further specific examples (IT): (1) A law regulating advanced electronic signatures which pre-dates eIDAS has not been repealed. It requires entities providing advanced electronic signature solutions to have, inter alia, an insurance policy to operate on the Italian market. - DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71. (13A04284) (GU Serie Generale n.117 del 21-05-2013)). Available at: <https://www.gazzettaufficiale.it/eli/id/2013/05/21/13A04284/sg>; (2) An Italian law on trust services and digital administration defines the FirmaSPID signature (linked to the SPID eID, an Italian notified eID scheme) as having the same legal validity as an advanced electronic signature. There are concerns that this may create difficulties for providers looking to compete with the entity offering it. - (DECRETO LEGISLATIVO 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale. (GU n.112 del 16-5-2005 - Suppl. Ordinario n. 93)). Consolidated version available at: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82>. (AT): A law requires that qualified certificate used for accessing online services provided by the public administration must contain a specific identification code, not reported on official documents of identification. This may create interoperability issues. Recital 54 of eIDAS notes that “the inclusion of specific attributes, such as unique identifiers, in qualified certifications should be allowed, provided that such specific attributes do not hamper cross-border interoperability...of qualified certificates...”

¹⁸⁷ InfoCert: eIDAS Review InfoCert Group Contribution to the revision process of the eIDAS Regulation (2019), p.6.

In Germany, trust services seem to be underused in the daily work of public administration. To address this issue, existing regulatory gaps in German law could be closed. In fact, several eIDAS tools have not yet been implemented, in particular the electronic seal and the qualified certificate for website authentication. For instance, for the certification of documents which is one of the most frequent requests by citizens addressed to public administration, under current law, the public administration must be able to produce electronic attestations from self-issued certificates. However, the administration law only provides in that regard for the use of a qualified electronic signature and requires additional information on the identity of the issuing authority. If the law also provided for the use of an electronic seal, this additional information would not be needed as the identity of the issuing authority would have already been verified via the electronic seal.¹⁸⁸ Other stakeholders noted that, in some Member States, the public sector has created their own parallel instruments.

Q17. Are there overlaps or complementarities between the eIDAS Regulation and any other Community actions, which share objectives?

The Regulation plays an enabler role in the sectoral EU legislation with reference to eIDAS based solutions that provide legal effect and the assurance of compliance for the concerned entities (e.g. obliged entities in the AMLD or third party payment service providers covered by PSD2) against the obligations or requirements governed by these initiatives. The provision of the eIDAS services is often linked to the services covered by these EU initiatives and provides additional incentives for the service providers to obtain the eIDAS compliance status.

Anti-Money Laundering

Anti-money laundering legislation aims to prevent the financial system from being used for money-laundering and the financing of terrorist activities. Certain amendments have been made to the regime to cater for the legal framework put in place by the eIDAS Regulation. For example:

- Article 13(1)(a) of Directive 2015/849/EU¹⁸⁹ which establishes that customer due diligence comprises identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source (Know Your Customer), has been amended by Directive 2018/843/EU¹⁹⁰ so that electronic identification means and trust services within the meaning of the eIDAS Regulation constitute such a source.
- Article 27(2) of Directive 2015/849/EU requiring obliged entities to take adequate steps to ensure that 3rd parties provide data regarding the identity of a customer or its beneficial owner extends (by virtue of Directive 2018/843/EU) the obligation to data obtained through eID means and relevant trust services pursuant to the eIDAS Regulation. Similarly, Article 40(1) extends (by virtue of Directive 2018/843/EU) the requirement to retain data necessary to comply with due diligence requirements to information obtained through eID means and relevant trust services pursuant to eIDAS.

¹⁸⁸ Manfred Klein, "Studie der Bundesdruckerei zur eIDAS Verordnung – eIDAS muss gesetzlich stärker berücksichtigt werden", 10.9.2019, available at: <https://www.egovernment-computing.de/eidas-muss-gesetzlich-staerker-beruecksichtigt-werden-a-863442/> (last accessed on 17.12.2019).

¹⁸⁹ Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation 648/2012/EU of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73–117.

¹⁹⁰ Directive 2018/843/EU of the European Parliament and of the Council of 30 May 2018 amending Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, p. 43–74.

- 2(c) of Annex III of Directive 2015/849/EU is amended so that electronic identification means and relevant trust services as defined by the eIDAS Regulation are explicitly mentioned as a form of safeguard where non-face-to-face transactions are concerned.

The abovementioned instruments are Directives, meaning they require effective and accurate transposition into national law. Thus, it is possible that a major source of incoherence between the eIDAS Regulation and the anti-money laundering regime is inadequate transposition of the requirements related to electronic identification means and relevant trust services into national law. It should be noted that, as of 2 June 2020, 4 Member States had yet to notify transposition measures, while several others had notified only partial transposition, despite the deadline for transposition being 1 January 2020.¹⁹¹

Financial institutions apply several AML requirements identified in local AML legislation which are developed in line with the FATF Recommendations.¹⁹² They tend to require the following identity attributes: Name, address; date of birth; nationality; place of birth; gender; email address; occupation. If the datasets are not aligned to eIDAS dataset¹⁹³, they may need to request additional information.

The FATF's recently published Guidance on Digital Identity¹⁹⁴ notes that while the interpretative note describes such interactions as potentially *higher risk* situations, 'this statement does not require appropriate authorities and regulated entities to always classify non-face-to-face business relationships or financial transactions as higher risk for ML and TF purposes. It goes on to state that, given the evolution of the technology, it is important to clarify that non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a *standard level of risk*, and may even be *lower-risk* where, inter alia, higher assurance levels are implemented. This should help to provide clarity for entities in the financial sector, regarding the role of eIDs in their customer due diligence risk assessment. Although it is only a few months since publication, this guidance may alleviate concerns about using eIDs in the on-boarding process, particularly in relation to those with high assurance levels. Nonetheless, this does not solve the issue of alignment of the data set in the eID with the data needs of the financial institution. One possibility explored in the interviews which could solve this alignment issue is the move towards attributes assertion, whereby the user could assert certain attributes which are needed for certain sectors.¹⁹⁵

Payment services

Recital 95 of Directive 2015/2366/EU¹⁹⁶ notes the fundamental importance of security of electronic payments to the protection of users and the development of a sound environment for eCommerce. Article 4(30) defines "strong customer authentication" as "authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data." Article 97 of Directive

¹⁹¹ https://ec.europa.eu/info/publications/anti-money-laundering-directive-5-transposition-status_en

¹⁹² Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU, PwC 2018, p.23.

¹⁹³ The minimum data set for eIDAS is set out in Annex to Commission Implementing Regulation (EU) 2015/1501.

¹⁹⁴ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf>

¹⁹⁵ It should be noted that the respondents to the trust service provider survey were divided on whether eIDAS was coherent with PS2 and AML4 provisions, while the majority of respondents to the survey aimed at supervisory bodies, conformity assessment bodies and national accreditation bodies remained neutral on this question.

¹⁹⁶ Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation 1093/2010/EU, *OJ L* 337, 23.12.2015, p. 35–127.

2015/2366/EU requires payment service providers to apply strong customer authentication where certain conditions are met (i.e. account accessed online, electronic payment transaction initiated, any action through a remote channel which may imply a risk of payment fraud). Article 98 states that the European Banking Authority (EBA) shall develop draft regulatory technical standards addressed to payment service providers, specifying the requirements for strong customer authentication. On the basis of the draft regulatory technical standards drafted by the EBA, the Commission adopted Delegated Regulation (EU) 2018/389.¹⁹⁷

While Directive 2015/2366/EU makes no explicit mention of the eIDAS Regulation, the delegated regulation notes in recital 27 that to improve user confidence and ensure strong customer authentication, the use of electronic identification means and trust services as set out in the eIDAS Regulation should be taken into account, in particular with regard to notified electronic identification schemes. Article 34(1) of the delegated regulation provides that, for the purpose of identification, as referred to in Article 30(1)(a)¹⁹⁸, payment service providers shall rely on qualified certificates for electronic seals or for website authentication.

Thus, some coherence between the EU legislative framework on payment services and the eIDAS Regulation is ensured via the supplementation provided by the delegated regulation. While the manner in which the provisions of Directive 2015/2366/EU apply in the Member States depends to an extent on their transposition, the provisions of Commission Delegated Regulation (EU) 2018/389 apply directly, which removes a potential obstacle to coherence between the legal framework for payment services and the legal framework for electronic identification and trust services.¹⁹⁹ One stakeholder raised a coherence issue between the eIDAS Regulation and the PSD2 Directive with regard to the way legal persons are identified. The eIDAS Regulation includes in its Minimum Data Set the Legal Entity Identifier (LEI). However, this attribute is only optional at the moment, making it impossible to rely solely on this information to identify a legal person in Europe. The PSD2 directive has introduced a licensing regime for payment initiation and account information service providers, altogether referred to as Third Party Providers (TPPs) that is administered by National Competent Authorities (NCA). This number (TPP licensing number) must be included in the eIDAS compliant PSD2 certification used by the TPPs as a specific attribute. As a result, such certificate cannot be reused for any other digital transaction as they are customised to this PSP identifier. This situation does not ensure a full interoperability of the system and clearly collides with the objectives of rolling-out the Once-only principle across Europe.

Use of digital tools and processes in company law

Directive 2017/1132/EU²⁰⁰ codified the provisions related to the establishment and functioning, and cross-border mergers of limited liability companies. Directive 2019/1151/EU amends it by replacing Article 13,²⁰¹ with specific provisions on the recognition of electronic identification means in relation to online procedures related to registers. Notably, it provides that Member States

¹⁹⁷ Commission Delegated Regulation 2018/389/EU of 27 November 2017 supplementing Directive 2015/2366/EU of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, *OJ L 69*, 13.3.2018, p. 23–43.

¹⁹⁸ which provides that account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments be able to identify themselves towards the account servicing payment service provider.

¹⁹⁹ While closed communities, such as bank to bank services are outside the scope of the Regulation, the requirements of Directive 2015/2366/EU may nonetheless lead many banks to use eIDAS trust services for customer-to-bank interactions – see Thales, “The impact of the European eIDAS Regulation- Understanding the new requirements and the need for hardware security modules”, White Paper.

²⁰⁰ Directive 2017/1132/EU of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, *OJ L 169*, 30.6.2017, p. 46–127.

²⁰¹ Directive 2019/1151/EU of the European Parliament and of the Council of 20 June 2019 amending Directive 2017/1132/EU as regards the use of digital tools and processes in company law, *OJ L 186*, 11.7.2019, p. 80–104.

must recognise eID means issued in another Member State and recognised for the purpose of cross-border authentication pursuant to Article 6 eIDAS Regulation. However, it sets out an exception to the obligation if the assurance level of such electronic identification means do not comply with the conditions of Article 6(1).

Directive 2019/1151 inserts a transparency requirement, whereby Member States need to ensure that all identification means recognised by Member States are made publicly available. However, recital 10 clarifies that Member States should be free to determine the way in which the identification means which they recognise, including those which do not fall within the scope of the eIDAS Regulation, should be made publicly available. In principle, if an eID scheme is notified in accordance with eIDAS Regulation, and published by the Commission pursuant to Article 9 thereof, any person should be able to consult the list to check the assurance level of the scheme, then consult the eID means required by the public body and check the assurance level. In this way, the person can ascertain which eID means the public body is obliged to recognise pursuant to Article 6(1) eIDAS Regulation. However, this does not tell the person:

- Which eID means the public body recognises in practice (perhaps the public body is not in compliance with Article 6(1) eIDAS Regulation); or
- Whether, notwithstanding the non-satisfaction of the conditions set out in Article 6(1) eIDAS Regulation, the eID means are accepted by the public sector body (if the public sector body accepts eID means with a lower assurance level, this is only useful to a person using such means if they are aware of this).

Although this obligation to make publicly available is limited to the realm of company law, it may be a useful from the perspective of increasing awareness and legal clarity for users of eIDs.

Finally, Directive 2019/1151/EU allows Member State to require the physical presence of the bearer of an eID, if a three-fold test is satisfied:

- It is justified by reason of the public interest in preventing identity misuse or alteration;
- The physical presence can only be required on a case-by-case basis, where there are reasons to suspect identity falsification; and
- Any other steps of the procedure can be completed online.

It should be noted that there is no such corresponding provision in the eIDAS Regulation. However, the eIDAS concerns the recognition by public sector bodies of eID means from other Member States. However, identity fraud is something which can occur in relation to both eID means issues within that Member State or in another Member State (and benefiting from mutual recognition). It seems reasonable to provide for the possibility of measures being taken where there is a reason to suspect fraudulent practices. However, it is essential that such a provision is drafted and executed in a non-discriminatory manner (as referred to in Article 12 (3) (a) of eIDAS Regulation). Thus, it should not treat eID means issued in other Member States differently to eID schemes issued the Member State where the fraud is suspected.

European citizens' initiatives

Regulation (EU) 2019/788²⁰² establishes the procedures and conditions required for the European Citizens' Initiative. This is not an internal market instrument but rather, having Article 24 TFEU as its legal basis, is intended to increase democratic participation in the EU. Article 9(2) of Regulation (EU) 2019/788 requires that when notified eIDs are being used, citizens must provide their nationality in addition to the minimum dataset set out in Annex to the Commission Implementing

²⁰² Regulation 2019/788/EU of the European Parliament and of the Council of 17 April 2019 on the European citizens' initiative, *OJ L 130, 17.5.2019, p. 55–81*.

Regulation (EU) 2015/1501. Thus, as nationality is not included in the minimum dataset, the citizen is currently required to manually enter their nationality in addition to the identification with their eID. Inclusion of nationality within the minimum dataset could remove this issue. This issue is currently being considered by the eIDAS Technical Subgroup and the Cooperation Network, but no conclusions have thus far been reached in this regard.

Single Digital Gateway Regulation (SDGR)

Recital 21 of Regulation (EU) 2018/1724²⁰³ notes that it should build on the eIDAS Regulation. Article 6 of the SDGR requires Member States to ensure that users can access and complete certain procedures (set out in Annex II) fully online. This is subject to the qualification that the relevant procedure has been established in that Member State. It goes further and defines what “fully online” should be understood to mean, part of which is that “the identification of users, the provision of information and supporting evidence, signature and final submission can all be carried out electronically at a distance...”. This obligation shall apply by 12 December 2023.

Further, Article 13(2)(c) provides that Member States shall ensure that cross-border users are able to identify and authenticate themselves, sign or seal documents electronically, as provided for by the eIDAS Regulation, in all cases where this is possible for non-cross-border users.

The obligations imposed by the SDGR are slightly different to those imposed by the eIDAS Regulation. While the latter imposes an obligation to recognise trust services and electronic identification means, the former focuses on the access to and use of the online procedure by the user and the making available of the procedure by the Member State. For example, Article 6(1) of the eIDAS Regulation imposes an obligation on public sector bodies to recognise electronic identification means issued in another Member State for cross-border authentication provided certain conditions are met. Article 13(2)(c) SDGR, on the other hand, puts the cross-border user at the centre of the obligation on the Member State, rather than the electronic identification means themselves.²⁰⁴ The distinction is subtle, but important. It may be the case that electronic identification means or an eSignature is recognised by the public authority providing a public service, but in practice the user cannot avail of the service for some other reason (e.g. when they enter their contact details, the national prefix of their phone number is not recognised). The SDGR aims to resolve such situations. Thus, taken together, the SDGR and the eIDAS Regulation are capable of being mutually reinforcing.

Article 14 of the SDRG Regulation on requirements for the once only technical infrastructure also relies on the provision of cross border electronic identification in accordance with the eIDAS Regulation, although only indirectly implied as a pre-requisite for the exchange of evidence but nevertheless essential in order to match an identity with an evidence.

Cross-border healthcare

Recital 10 of the eIDAS Regulation refers to Directive 2011/24/EU on cross-border healthcare,²⁰⁵ which set up a network of national authorities responsible for e-health. Article 14(2)(c) gives the network the objective of supporting Member States in “developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare”. Recital 10 notes that mutual recognition of electronic identification and authentication is key to making cross-border healthcare for European citizens a reality, and that this requires a safe, solid and trusted

²⁰³ Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.), PE/41/2018/REV/2, OJ L 295, 21.11.2018, p. 1–38.

²⁰⁴ Article 3(2) SDGR defines a “cross-border user” as “a user in a situation, which is not confined in all respects within a single Member State”.

²⁰⁵ Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45–65.

electronic identification framework. Thus, the eIDAS Regulation can act as an enabler for the rollout of electronic healthcare solutions.

Again, no coherence issues have been identified between this directive and the eIDAS Regulation. The directive does not refer to the eIDAS Regulation and pre-dates it by several years. It was noted in 2018 that, regarding patient and healthcare professionals' identification, as well as access rights to electronic health records, there is also a significant variety of available systems and approaches across the EU Member States. Thus, Directive 2011/24/EU might benefit from a more explicit link to eIDAS. This could, for example, consist of clarifying that notified eIDs are presumed to provide adequate identification and authentication for the purposes of cross-border healthcare. Indeed, there may be a consideration as to whether a certain assurance level (e.g. high) might be required, due to the particularly sensitive nature of health data. Of course, the level of coherence between eIDAS, EU healthcare legislation and the GDPR may hinge on the issue of the minimum data sets provided for pursuant to eIDAS. On the one hand, the healthcare sector may require more data than the minimum data set. On the other hand, health data is a special category of personal data pursuant to Article 9 GDPR, making it subject to more stringent rules on processing. Article 9(4) provides the possibility of Member States maintaining or introducing further conditions, including limitations, with regard to the processing of such data. A solution could be the inclusion of attributes which could be asserted for given sectors (such as health), but not transmitted in relation to other interactions which the user of the eID has (for example, completing his tax return). This could enable sufficient data to be transmitted to healthcare providers to make the eID attractive in that sector, without sharing sensitive personal data with other actors. It could also provide a more secure environment for the secondary use of health data, by enabling seamless access to medical registries to strongly identified researchers.

General Data Protection Regulation (GDPR)

The eIDAS Regulation makes clear in Article 9 that the interoperability framework shall facilitate the principle of privacy by design and ensure that personal data is processed in accordance with EU data protection law. In order to ensure uniform conditions for the implementation of the interoperability requirement, Article 12(8) provides for the adoption of implementing acts by the Commission. It adopted Implementing Regulation (EU) 2015/1501, which sets out, inter alia, the following minimum data set for natural persons:

1. current family name(s);
2. current first name(s);
3. date of birth;
4. a unique identifier 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.

The minimum data set for a natural person may contain one or more of the following additional attributes:

1. first name(s) and family name(s) at birth;
2. place of birth;
3. current address;
4. gender.

There are two issues to consider when reviewing the minimum data set. Firstly, it should be considered whether it satisfies the data minimisation principle, meaning that the data are 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are

processed'.²⁰⁶ Secondly, the explicit requirement of data protection by default, which requires data controllers implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.²⁰⁷

The departure point for both issues is an appreciation of what is necessary and what the purpose of the processing is. Article 3(1) of eIDAS defines electronic identification as 'the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person,' while person identification data is defined as 'a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established. To the extent that the purpose of electronic identification is to ensure the identity of a particular person in the same way as a national identity card would, when dealing with a public body such as a tax authority, this minimum data set would seem to correspond to the information which the tax authority needs in relation to taxpayers. In that sense, its processing in the context of a tax return may be necessary.

However, viewed in light of the assertion in recital 17 of eIDAS regarding the encouragement of private sector use, it should be considered whether this minimum data set is necessary for the various interactions which an individual may be expected to have in the private sector. For example, if a natural person wishes to use his eID in order to prove majority in the context of purchasing alcohol or cigarettes or accessing gambling services, it may not be necessary for the service provider to know his address or even name and date of birth (only that it is a date more than 18 years from the day of transaction). Thus, there may be different considerations regarding necessity of data processing when a more widespread use of eID is made in the private sector. If the processing of only certain data from the data set is necessary in order to access a service, it should be considered whether a setup based on the transmission of that entire data set is coherent with the GDPR's principle of data protection by default.

On the other hand, it has been noted that certain sectors (such as health or finance – sex could be an important health parameter, in the latter, banks may require the nationality of the individual as part of KYC check) may have a need for certain additional attributes in the data set. This represents an additional challenge in relation to the concept of minimum data set in the current implementing act. Expanding the minimum data set to include additional data required for such sectors would seem inconsistent with the abovementioned principles of data protection law unless the data to be transmitted were different depending on the needs of the sector. Thus, the additional data that may be required by the health sector would not be included in the data transmitted in other sectors, which would enable the user of the eID to only share the data necessary for the interaction in question, while increasing the attractiveness of the eID for certain sectors.

EU digital and green deal policy agendas

The "Europe's Digital Decade: digital targets for 2030"²⁰⁸ Commission Communication states that digital technologies can significantly contribute to the achievement of the European Green Deal objectives. The uptake of digital solutions and the use of data will help in the transition to a climate neutral, circular and more resilient economy and digital technologies allow greener processes in services. Among the main objectives of the Regulation was to reduce administrative burden and move towards paperless transactions given the increased use of electronic transactions as well as increased quality of services. The increase in use of eIDAS based solutions during the COVID-19 pandemic has particularly highlighted the importance of the framework for the digital interactions

²⁰⁶ GDPR, article 5(1)(c).

²⁰⁷ GDPR, article 25.

²⁰⁸ COM(2021) 118 final

not only in the public sector. For example, the number of users of the notified Italian eID (SPID) has tripled between January and December 2020 (5m – over 15m).

5.5 EU added value

Q18. Is there additional value (at national, European and international level) resulting from the eIDAS Regulation, compared to what could be achieved with similar regulatory frameworks at national level?

Stakeholders consulted largely agreed that the eIDAS Regulation has created an added-value compared to what could have been achieved with similar regulatory frameworks at national level. The eIDAS Regulation is considered by many as the most advanced framework in its field, also in an international comparison. The existence of this common framework makes it unnecessary for business to develop own and sector-specific solutions with substantial benefits in legal certainty and cost reduction associated.

Trust Services

The eIDAS Regulation provides a common legal framework for the use of trust services, effectively reducing the fragmentation of the market and fostering interoperability of solutions. Public administrations have been able to modernise and digitise a large part of their services and evidence issuance thanks to eSignature and eSeals. Digital transformation of public administration also reduces administrative burden. The issuance of digital evidence based on eSeals supports the roll-out of the Once-Only principle across the EU. The security of online public and private services have been improved with the use of website authentication.

eID

Regarding electronic identity, the assessment of EU added-value needs to be more measured. For eID, the eIDAS Regulation has not reached the expected results to provide a secure digital identity to all EU citizens. However, stakeholders agree that eID/eIDAS has been instrumental for Member States to integrate digital identification into their respective eGovernment strategies and to recognise it as a key enabler for the digital transformation of public administration. However, the effective uptake and use of notified eID schemes for cross-border transactions remains low.

The parallel development of sector-specific solutions for the private sector in some cases was caused by the immature design of the regulatory framework that focused on the public sector. Translation of the theoretical EU added value for the public sector was hampered because complementary regulatory frameworks as well as technological solutions assuring the ability of users to complete a procedure (e.g. once-only-principle) was missing, therefore, the need did not turn into demand.

Stakeholders suggest that the scope of the eIDAS Regulation should be extended to provide a legal framework for all types of electronic identity scheme and foster the portability of identity attributes.

It was also mentioned that awareness is a decisive factor to increase take-up and legislative action should be taken to improve interoperability and reach within the private sector.

Q19. To what extent do the issues addressed by the eIDAS Regulation require further action at EU level? Which recommendations can be made to improve EU added value?

The need for trust and security of digital transactions is increasing. The digital transformation of the economy and European public administration is accelerating, driven by the potential benefits in terms of administrative burden reduction and increased quality of services (e.g. mobile access to online services, once-only principle and improved user experience).

Both in the field of electronic identity and trust services, stakeholders are advocating an extension of the scope of the eIDAS Regulation to cover more use cases in particular in the private sector. As

the assessment of other evaluation criteria shows, a number of issues require further action at EU level to improve EU added value. These include:

- **Verifiable Claims:** Create a legal framework for the issuance and the exchange of verifiable claims and enable a user-centric framework that allows control of personal data and supports new innovative business models linked to digital identity;
- **GDPR Alignment:** Integrate concepts of data minimisation and zero-knowledge claims in order to align with, and support the implementation of the GDPR;
- **Sector-specific Attributes:** Facilitate the adoption of sector-specific attributes to foster the reuse of eIDAS eID. The current system does not offer a general foundational ID scheme that could replace functional identity management systems created in various areas;
- **Private Sector Focus:** Clarify the commercial model and liability rules to foster the reuse of notified eID schemes by private service providers;
- **Awareness:** Take measures to increase awareness about eIDAS and its potential benefits;
- **New Trust Services:** Adopt new trust services e.g. to support use cases linked to the development of Distributed Ledger Technology and blockchain technology;
- **Increase Harmonisation:** Address barriers to the uptake of trust services resulting from national interpretation of the eIDAS Regulation and/or conflicting national law. - More than 70% of trust service providers and supervisory bodies considered that there are areas of the eIDAS Regulation that requires further harmonization and more than half consider that the supervision of trust service requires further intervention at the European level.

Q20. What would be the most likely consequences of repealing the eIDAS Regulation?

Before the entering into force of the eIDAS Regulation, the markets for eID and trust services in Europe were fragmented and there was no single tool for cross-border authentication across the EU. Stakeholders agreed that a repeal of the eIDAS Regulation would result in fragmentation of the European identity and trust services market given that the eIDAS Regulation provides a legal framework for secure digital transactions.

eIDAS has created mutual recognition for digital identification and trust services across Europe and several sectorial EU legislations (e.g. PSD2, AMLD, Company Law etc.) include cross-references to the eIDAS solutions to ensure compliance with the legal requirements set out in these regulatory frameworks. Repealing the eIDAS Regulation would have negative consequences in other regulatory environments that rely on the eIDAS Regulation. Without eIDAS, other solutions would have to be developed for these sectors, which would likely be sector-specific and thus jeopardising synergies and reducing economies of scale, in addition increasing the administrative burden where citizens and businesses are subject to more than one regulatory scheme. Stakeholders believe that rather than repealing it, the eIDAS Regulation should be improved and expanded.

6. CONCLUSIONS

Overall, the eIDAS Regulation has contributed positively to the further development of the Single Market. It has provided the foundations for the development of an identity and trust services market in the EU, supporting the ever-increasing need for secure digital transactions. However, in a future-looking perspective, which has evolved as regards objectives and user-expectations in a society that has had an unprecedented digitalisation push due to the COVID pandemic, it would deserve a number of improvements in terms of effectiveness, efficiency, coherence and relevance to deliver on the new objectives and under new circumstances.

The absence of a mandatory notification, the complex system of interoperability and the limited minimum data set rely on the design of the eIDAS Regulation, which disincentivise or make more difficult implementation. Lack of demand for cross-border public services transactions is independent from eIDAS. The COVID pandemic has shown that cross border demand for public and private services will become more important. New needs by the private sector (strong

identification means for the financial, aviation, health or education sector for example) both for eID systems and for new trust services (such as attestation of attributes of identity linked data) are also independent from the Regulation.

The complexity of the current interoperability architecture, means that the mutual recognition of eID schemes across borders remains mainly possible in theory. In practice, very few users manage to effectively proceed to cross-border authentication. Some key barriers to the full coverage of the EU population and uptake in the private sector have prevented the regulatory framework to reach its full potential. The current limited scope and focus of the eIDAS Regulation on eID schemes notified by EU Member States and access to online public services seems inadequate. The vast majority of the needs of electronic identity and remote authentication currently reside in the hands of the private sector, notably for stakeholders like banks, telecom and platform operators that are required by law to verify the identity of their customers. The case of a citizen wanting to access an online service in another Member State is in the end a very narrow scope and represents a minimum number of use cases that does not necessarily justify the current costs of the overall set-up and operations of the network.

The absence of a commercial model for private identity providers and the lack of clarity of the terms and conditions of access to the eIDAS network for private relying parties are major blocking factors to the long-term maturation of the regulatory framework. Our overall conclusion is that more fundamental changes need to be made to the eIDAS Regulation to support the use cases for identification required by the private sector.

Some important modifications could take place in the form of a revision of the current regulatory framework. This would include the definition of trust services supporting the provision of additional attributes and remote authentication verification procedures, among others.

The provision of digital identity could be based on a principle of certification, where Member States could become authoritative sources for a series of legal identity attributes, while private sectors stakeholders could also become attribute providers for additional attributes for specific use cases. The functions of attribute provider, identity providers, identity broker, authentication providers could be clearly differentiated. In this scenario, the portability of identity credentials could be better supported, reducing the multiplication of identity verification procedures that are time consuming for citizens and businesses as well as costly for the service providers subject to such mandatory verifications. The mandatory acceptance of digital credentials respecting eIDAS requirements by public and private relying parties could be introduced. This approach, would enable to system to be more open to innovation and scale-up.

For each identification, eID under eIDAS transmit a minimum data set, which includes first name(s) and family name(s); date of birth and a unique identifier (as persistent as possible in time). This minimum data set is compulsory for cross-border authentication to access online public services. Data protection by design and by default is actively built into eIDAS through the minimum data set, which is the only data transmitted in a transaction for the purpose of identification, considering that eIDAS only covers public services where the users must identify themselves; this minimum data-set is necessary for all transactions. The issue with the minimum data set is that it is rigid, and not always sufficient for specific transactions or services. There is no possibility for the user to add additional data that is necessary in order to access certain private sector services or to facilitate compliance with specific sectorial regulatory requirements. The number of cases for which notified eIDs can be used are therefore in practice limited. There is also no possibility for the user to limit the transmitted data to the minimum necessary for the authentication to a specific service. Access to certain services requires less data (for example to purchase alcohol one only needs to prove age). The implementation of the current eIDAS system does not allow the user to actively enforce the GDPR principles of data minimisation and privacy by default and to control which data to share and with whom.

On the side of trust services, the eIDAS framework has been more successful at establishing a European market for such solutions. Many stakeholders expressed their concerns with regard to the lack of harmonisation of certain dispositions. This situation leads to unfair practices and cherry-picking strategies that are eventually harming the overall trust that stakeholders are putting in the security and integrity of the eIDAS framework.

Many stakeholders have also called for formalising the current cooperation between the national Supervisory bodies. Contrarily to the creation of the eIDAS framework under Chapter II, there is indeed no official forum of discussion or exchange of best practices between national countries with regard to trust services at EU level. Most of the supervision is performed at national level, which reinforced this issue of fragmentation raised by some stakeholders and undermine the possibility to closely follow-up on technological developments and/or trends that could require an adaption of the regulatory framework for trust services. Non-regulatory guidance, adoption of implementing acts already foreseen in the Regulation, and minor regulatory intervention could help fix these fragmentation and governance issues.

In terms of relevance, the need to support remote identification and verification cases calls on the adoption of new trust services. Additional trust services such as the preservation of electronic signature, the digitisation of paper documents and identity for IoT devices could be considered.

Effectiveness

eID

The provisions on electronic identity have led to the creation of the eIDAS network, which enable holders of a notified eID scheme to access online public services across borders. The interoperability of a number of eID schemes has been achieved at EU level.

Despite these achievements, eID under eIDAS has not achieved its potential in terms of effectiveness regarding digital identity. Only a limited number of eIDs have been notified, limiting the **coverage** of notified eID scheme to about 59% of EU population. In addition, the **acceptance** of notified eIDs both at the level of Member States and service providers is limited, as not all eIDAS nodes are up and running and a limited number of public services offer eIDAS authentication. On the basis of available data it seems that only about half of the services accessible through domestic eID are connected to the national eIDAS infrastructure. There are not sufficient incentives to Member States and service providers to connect to the infrastructure and make cross-border authentication possible. The actual documented **use** of notified eID across borders is very limited - between few authentications to several thousands per month. The eIDAS framework lacks monitoring and reporting obligations which limits the access to reliable data on active connections and usage. Although the actual cross border use of eIDs is very limited, the evolution of the number of transactions in certain Member States confirms that the usage of notified eID schemes is increasing progressively since September 2018 as more and more eID schemes become available for cross-border use. Another factor limiting the use is a lack of awareness of eIDAS among citizens and the use of notified eIDs by private service providers. The largest part of the digital identity market is not covered by the eIDAS Regulation. Despite its initial objective, eID/eIDAS has not been able to expand sufficiently into the private sector, which is a key weakness. eID-enabled e-government applications are necessary to develop usage and to constitute a first user base, while it is only through private sector applications that frequent use and a high level of usage of eIDs can be achieved.

Some stakeholders recommend a radical **review of the notification and peer review procedures**. The current governance model established by the Regulation and the implementing acts would profit from further improvements and streamlining of the processes. Improving the peer-review processes of the pre-notified eID schemes within the Cooperation Network, introducing standardisation and certification of the components of the notified eID schemes by a dedicated supervisory body to demonstrate the compliance against the functional requirements set out by the

regulatory framework, could provide more clarity, enhance trust between the Member States and lighten the notification process. This way the governance of eID would be more aligned with the current governance of trust services, including audits, regular revisions, etc. Such a system already exists in countries that have adopted eID schemes based on a federation of identity providers²⁰⁹. Stakeholders think that a **harmonisation of certification** will bring more confidence and trust to stakeholders, and will clarify the eIDAS security requirements and LoAs.

Member States call for an agreement on the tools and procedure to manage eID related **incidents**. The current regulatory framework relies on the country that has notified an eID scheme to report security incidents and disconnect its system from the network. Member States and industry stakeholders call for an introduction of a **safeguard mechanism** to enable Member States to protect their infrastructure and suspend the acceptance of a scheme based on reasonable doubts and proof (in line with a set of pre-defined conditions).

Trust Services

The eIDAS Regulation has successfully established legal certainty on liability, burden of proof, legal effect and international aspects of trust services, but some issues remain. **Availability and take-up of trust services** in the EU have increased since the introduction of the eIDAS Regulation, however, there are differences among Member States and among different trust services.

The objective of the Regulation to remain technology neutral has led to a **diversity of interpretation of the requirements between Member States**. Most of the identified effectiveness issues raised by stakeholders concerns the lack of adoption of implementing acts already foreseen to be adoption by the current legal framework. As a result, it cannot be concluded that a level playing field has been fully achieved at EU level. However, the eIDAS Regulation has set-up a strong framework that can be complemented with the necessary standards and requirements to reduce the current fragmentation of the market and divergences of interpretation by supervisory bodies and conformity assessment bodies.

Most supervision is performed at national level, which reinforces this issue of fragmentation raised by some stakeholders and undermines the possibility to adapt the regulatory framework to technological development. Stakeholders are calling for a **formalisation of the cooperation between supervisory bodies** to improve implementation of the eIDAS Regulation.

The supervision model for the trust services could be improved and remove lack of harmonisation and ambiguities in some of the procedures, by adopting implementing acts with references to standards for the accreditation and conformity assessment processes and harmonisation of the scope and depth of conformity assessment reports. Improving cooperation between national supervisory bodies by establishing an official forum for coordination and the exchange of best practices with regard to trust services, similar to the eID chapter of the Regulation (i.e. the Cooperation Network) could be considered in the revision process.

Efficiency

eID

The key stakeholder groups for which the eIDAS Regulation has generated costs and benefits are national authorities, eIDAS node operators, eID providers and service providers. In charge of managing the system²¹⁰, national authorities and eIDAS node operators and eID Providers bear significantly higher costs than service providers.

²⁰⁹ e.g. SPID federation in Italy

²¹⁰ National authorities and eIDAS node operators and eID Providers deal with administrative costs derived from the notification process of eID schemes, the peer review process of other countries' eID schemes and the cooperation and communication activities with other Member States and the European Commission.

The baseline assessment indicates that quantifiable costs are higher than benefits. This is the result of a low uptake where benefits did not materialize. For individual stakeholders, a considerable part are expected benefits (discounted as future benefits) and therefore hardly quantifiable. Moreover, the evaluation identified three areas of intervention for possible net cost reductions: reducing uncertainty for the private sector, the centralization of the updates to nodes and outreach activity for final users.

Trust Services

The key stakeholder groups in the area of trust services for which the eIDAS Regulation has generated costs and benefits are accreditation, conformity assessment, and supervisory bodies and qualified and non-qualified trust service providers.

Recurring costs for governance are limited and mainly linked to ensuring compliance. In addition to compliance related activities, QTSPs spent an average of EUR 800.000,00 in order to qualify, be granted, and maintain the status of qualified trust service provider.

As for eID, the baseline assessment indicates that quantifiable costs are higher than benefits. For individual stakeholders, a considerable part of the benefits is only hypothetical at this stage (discounted as future benefits) and hardly quantifiable. Trust Service Providers register benefits in the form of revenue due to the provision of trust services in other EU countries and an extension of market base. This is also linked to a reputational increase and better access to finance due to compliance with the high standards of eIDAS Regulation.

The evaluation identified three areas of intervention for possible net cost reductions, including a greater harmonisation of supervisory activities, security requirements and a branding / PR campaign.

Relevance

eID

The eID ecosystem has profoundly changed since the introduction of the eIDAS Regulation with an increasing footprint of private identity providers. Taking into account the increase in digital transactions, all EU citizen should have access to a secure and interoperable digital identity, which is not the case today. Some key barriers to uptake by users and private sector service providers have prevented the regulatory framework to reach its full potential. The current scope and focus of the eIDAS Regulation on eID schemes notified by EU Member States and on enabling access to online public services seems too limited and inadequate. The vast majority of the needs of electronic identity and remote authentication remain with the private sector, in particular in areas like banks, telecom and platform operators that are required by law to verify the identity of their customers.

Despite introducing references to eIDAS solutions in a number of sectoral EU legislation, the eIDAS Regulation has not yet replied to the needs of specific sectors (e.g. education, banking, travel, aviation). One of the limitation factor of the current framework with respect to these sectoral needs is the lack of specific attributes by domains. There is a case for an extension of eIDAS with the provision of sector-specific attributes, identifying use cases and dedicating adequate resources to develop the respective data models. An introduction of new private sector digital identity trust services for identification, authentication and provision of attributes would support the issuance of verifiable claims and thus providing flexibility needed for the sectoral use cases.

Trust Services

The objectives of the eIDAS legal framework remain adequate to address the identified issues, notably the need to ensure the reduction of market fragmentation by ensuring cross-border and cross sector interoperability of trust services via the adoption of common standards. The key tension is the ability of eIDAS to stay in line with the latest development of technology in the domain of trust services. An update to the Commission Implementing Decision (EU) 2016/650

with the integration of the following two standards: CEN EN 419 241-2; CEN EN 419 221-5:2018 is already under discussion with the eIDAS expert group.

Another consideration is an extension of the trust services list, notably through the introduction of a trust service to enable the preservation of eArchiving, define requirements for the digitisation of paper documents and through the introduction of a list of trust services supporting portable identity credentials and decentralized identity (distributed ledger).

Coherence

Evidence collected shows that the eID part of the eIDAS Regulation is supported by a generally coherent system for mutual recognition of eIDs based on notification and peer review. In addition, the trust services framework provides for a coherent supervisory system for trust services. However, certain issues have been identified impacting the internal coherence of the Regulation.

eID

In relation to eIDs, the notification and peer review system set out in the eIDAS Regulation and implementing acts intended to deliver a common understanding of the level of assurance provided by an eID scheme. However, assessment of practical implementation shows that this is not always the case. The advantage of the framework set out in Chapter II (and the related implementing acts) is that it encourages flexibility and technological neutrality. However, a common understanding among Member States' experts what constitutes substantial and high is still missing.

The eID chapter also lacks a way for non EU-based eIDs to benefit from mutual recognition. The introduction of a provision similar to the current Article 14 which applies to trust services could be considered although the mechanism for achieving recognition of non-EU qualified trust services has not yet been exploited.

The focus on public services contrasts with the possibility for the user to limit the transmitted data to the minimum necessary for the authentication to a specific service as the minimum data set is always transmitted to allow the identification of a person. Access to certain services requires either less data or only certain claim, whereas in some cases additional attributes would be needed. The use of notified eIDs in the private sector would require reconsideration of when the minimum data set is necessary for the various interactions with an individual. The GDPR principles of 'privacy by design' and 'privacy by default' should allow users to limit the provision of digital identity attributes to what is necessary to receive a service in line with the general requirements of GDPR.

Trust Services

In relation to trust services, the rules on the assessment of the trust service providers against the functional requirements of the eIDAS Regulation to obtain the qualified status shows some weaknesses. Firstly, it provides a key role for conformity assessment bodies, but lacks sufficient detail on their obligations, liability or level of competence. There is a prevailing view that the quality of conformity assessment reports is variable and that there are differences among the various national supervisory regimes. Several stakeholders argue for the adoption of implementing acts wherever foreseen, and more reliance on standards, as this could deliver more harmonisation and prevent a regulatory race to the bottom.

The evaluation also identified some areas where divergent approaches at national level with impacts on trust and a level playing field. One example is Article 24(1)(d) which allows Member States to recognise certain identification methods (such as biometric verification) at national level. Furthermore some national rules require the presentation of a physical identity card in certain contexts, or cases where a fiscal authority may only accept a qualified electronic signature issued by a trust service provider established in its own Member State.

A number of other Regulations at EU level explicitly refer to eIDAS trust services and electronic identification as a reliable and independent source, such as AMLD5. However, one important shortcoming is the limitation of the eIDAS minimum dataset²¹¹ and the ineffectiveness of the procedures established to extend it. To date, it has not been possible to include essential information to enable the use of eID/eIDAS in various sectoral contexts, such as eHealth, transport or finance.²¹²

EU added value

eID

The eIDAS Regulation has created incentives for Member States to deploy an eID solution. The added value of the eIDAS Regulation with regard to electronic identity is limited due to its low coverage, uptake and usage. The needs originally identified for the creation of the eIDAS Regulation still remain relevant. Repealing the eIDAS Regulation would lead to fragmentation and negative consequences to other legislative areas that rely on eIDAS. Some adaptations to the regulatory framework could increase the EU added value of the eIDAS Regulation. Recommendations include to integrate concepts of data minimisation and zero-knowledge claims, to adopt sector-specific attributes to foster the reuse of eIDAS eID across all domains, to include trust services for trusted entity to verify attributes and to clarify the commercial model and liability rules. The absence of a commercial model for private identity providers and the lack of clarity of the terms and conditions of access to the eIDAS network for private service providers are major blocking factors for the regulatory framework to achieve its objectives.

Trust Services

The eIDAS Regulation has provided a common legal framework for the use of trust services, reducing fragmentation of the market and fostering the uptake of trust services. With the help of trust services, public administrations are able to modernize and digitalise services and issue evidence digitally thereby reducing administrative burden. Some barriers resulting from national interpretation and/or conflicting national law still remain and limit the uptake of trust services.

²¹¹ Provided for in Annex to Commission Implementing Regulation (EU) 2015/1501.

²¹² For example, entities in the financial services sector (for AML purposes) or the healthcare sector (for information about patient health) may need information which is not contained in the minimum dataset.

ANNEX 1: PROCEDURAL INFORMATION

Lead DG, Decide Planning/CWP references

The evaluation has been coordinated by the European Commission's Directorate-General (DG) for Communications Networks, Content and Technology supported by an interservice steering group (ISG) involving representatives of most of the European Commission DGs. The group steered and monitored the evaluation's progress and ensured that it met the necessary standards for quality, impartiality and usefulness.

Organisation and timing

The Inter-service Steering Group was set up to assist in the preparation of the evaluation. The invitation to appoint representatives was sent to all the DGs. The first meeting of the Inter-Service Steering Group took place on 5 September 2019 and the last one on 15 December 2020.

The evaluation roadmap was published on 27 September 2019 and feedback on this roadmap was received until 25 October 2019. The stakeholder consultation strategy was prepared and made publicly available on 21 July 2020²¹³. It set a number of consultation activities comprising an open public consultation, targeted consultations in the form of interviews and surveys and workshops. The open public consultation was launched on 24 July 2020 and ended on 2 October 2020. To maximise the response rate, the consultations activities were promoted at the Commission Digital Single Market portal, the eIDAS Observatory web space and via social media accounts on Twitter. The public consultation triggered 318 responses. The evaluation built on a series of 14 strategic interviews with individuals and organisations that provided strategic input for the definition of the data collection strategy and questionnaires and 27 targeted interviews with different types of stakeholder helping to investigate the issues identified through desk research and strategic interviews in further detail and more targeted manner. In total, 804 stakeholders were targeted in for the specific stakeholders surveys to gather primary data and fill in data gaps identified by desk research. The dissemination strategy involved a diversity of channels used for dissemination, timely communication on the survey and its purpose, limited and clear requests to stakeholders and daily monitoring of responses. In January 2020, a workshop was organized with Members of the Cooperation Network.

Exceptions to the better regulation guidelines

The open public consultation lasted ten weeks, instead of the usual twelve, thanks to a derogation granted by the Secretariat General.

Consultation of the RSB

The Regulatory Scrutiny Board ('RSB') selected the evaluation of the eIDAS Regulation for scrutiny. An upstream meeting was held with the Board on 7 September 2020.

The meeting of the Regulatory Scrutiny Board took place on 17 March 2021. The outcome was a positive opinion, issued on 19 March 2021. The evaluation was revised to address the concerns pointed out in the opinion with comments 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.

²¹³ Some of the main consultation activities, incl. the OPC covered the evaluation of the eIDAS Regulation process and the initiative "Proposal for a European Digital Identity (EUid) and Revision of the eIDAS Regulation" PLAN/2020/8518

RSB COMMENTS	ACTIONS TAKEN
<ul style="list-style-type: none"> • The report should clarify what the Regulation was expected to have achieved by now, to provide a clearer point of comparison against which to judge the current situation. • The report should better distinguish between the reasons behind the limited uptake of eID schemes and the development of the trust services market. It should clarify whether it has been due to deficiencies in the design of the Regulation, insufficient Member State implementation or other factors. It should better explain what role security and liability concerns play. • The report should elaborate on the situation across Member States, and explain why a significant number of them have chosen not to notify national eID schemes under the eIDAS Regulation. 	<ul style="list-style-type: none"> • The state of play section includes additional elements on what the success should look like at this point in time in terms of the expectations and in line with the initial commitments of the Member States. • The baseline, analysis section and conclusion have been updated with additional explanations on the limiting achievements of the Regulation stemming from the design aspects, its implementation and other factors. The liability and security aspects have been further clarified in the analysis section for both – eID and trust services parts of the Regulation. • The incentives, reasons and design aspects of the regulatory framework related to limited number of notifications has been further elaborated in the analysis section.
<ul style="list-style-type: none"> • The report should deepen the analysis of the continued relevance of the Regulation in view of evolving user needs and technological and market developments. • The report should be clearer on the actual and potential demand for cross-border eID and how it may differ across different user segments (e.g. public services, (semi-) regulated sectors, pure private online transactions). It should clarify to what extent eIDAS versus pure market-led schemes could play a role in meeting these demands. 	<ul style="list-style-type: none"> • The relevance of the regulatory framework, in particular the assessment of its initial objectives against the need for the future adaptations in line with the technological developments, evolved user’s needs and change of context have been further elaborated throughout the whole report. • The analysis section includes additional elements on the potential demand and cross-border uses cases.
<ul style="list-style-type: none"> • The report should draw clearer conclusions on how future proof the Regulation has been and how far its design and implementation has been able to accommodate fast-paced technological progress in digital ID technologies and changing user needs. 	<ul style="list-style-type: none"> • The conclusion section has been strengthened with additional conclusions on how the future proof the regulatory framework is and what improvements it would merit based on complementary explanations in the analysis section in light of the technological developments, evolved user’s needs and change of context.
<ul style="list-style-type: none"> • The report should better assess the coherence between the eIDAS Regulation and the General Data Protection Regulation (GDPR). It should better analyse the extent to which the eIDAS Regulation complies with the GDPR’s “privacy by design” and “privacy by default” requirements, in particular for potential use of the electronic identification by the private sector. 	<ul style="list-style-type: none"> • The conclusion section further elaborates on the coherence between the current regulatory framework and its compliance with the GDPR principles and what limitations this implementation entails for the extended uses cases in the future.

Evidence, sources and quality

The evaluation of the eIDAS Regulation was carried out between September 2019 and December 2020. It builds on evidence collected by an external support study²¹⁴ and draws on data from various sources, including the following studies, reports and sources that have been taken into account:

1. Electronic Identification and Trust Services for SMEs
2. Study on eID and digital on-boarding
3. Study on a marketing plan to stimulate the take-up of eID and trust service for the Digital Single Market
4. Feasibility study on cross-border use of eID and Authentication Services (eIDAS compliant) to support student mobility and access to student services in Europe
5. EU-wide digital Once-Only Principle for citizens and businesses Policy options and their impacts
6. STORK eID infrastructure as an enabler of cross-border efficiencies when interacting with public and private sectors
7. Feasibility study on an electronic identification, authentication and signature policy (IAS)
8. eSignature - Study on the supply side of EU e-signature market - Final Study Report by Formit
9. EU online Trustmarks – Building Digital Confidence in Europe
10. Study on the legal and market aspects of eSignatures
11. Study on Cross-Border Interoperability of eSignatures 2010

²¹⁴ Study SMART 2019/0046 evaluating the European Regulation 910/2014 (eIDAS Regulation) has been commissioned by the European Commission Directorate-General for Communications Networks, Content and Technology H4 (DG CNECT H4) and performed by Deloitte , VVA, Spark and ECORYS

ANNEX 2: STAKEHOLDER CONSULTATION

1. Introduction

This annex summarises the results of all of the consultation activities undertaken as part of the evaluation of the Regulation 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 and repealing Directive 1999/93/EC (the eIDAS Regulation).

Article 49 of the eIDAS Regulation requires the Commission to review the application of the Regulation, in particular whether it is appropriate to modify the scope of the Regulation or its specific provisions, taking into account the experience gained in the application as well as technological, market and legal developments, and report to the European Parliament and to the Council by 1 July 2020. In its Communication on Shaping Europe's Digital Future, published on 19th February 2020, the Commission took the position that universally accepted public electronic identity (eID) is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them²¹⁵. Consequently, the Commission has committed to revising the eIDAS Regulation to improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans. Consultation for the evaluation and revision of the eIDAS regulation have been conducted in a single exercise.

2. Consultation scope and objectives

The consultation activities aim at collecting views from all relevant actors in the implementation of the eIDAS Regulation, on the demand or the supply side of digital identity solutions, and from the general public. Different consultation activities were undertaken to make sure that all relevant stakeholder groups are appropriately engaged and consulted on their views and relevant questions.

The overall objectives of the consultation activities were twofold:

- to collect views, data and evidence on the implementation of the eIDAS Regulation to inform the evaluation of the eIDAS Regulation, and
- to collect views, data and evidence on the impacts of the alternatives for the revision of the eIDAS Regulation and for delivering an EU digital identity in order to support the Commission's assessment and choice of regulatory options for this initiative.

With regard to the **evaluation of the eIDAS Regulation**, the consultation activities sought to obtain feedback on the five evaluation criteria (effectiveness, efficiency, consistency, relevance, EU-added value), identify gaps, challenges and opportunities as well as collect views, evidence and data on how to remedy gaps, challenges or how to build on opportunities. Stakeholders participating in the implementation of eIDAS were asked to share views, evidence and data on the **costs and benefits** of the current eIDAS operating model and to identify areas where possible cost reductions could be made.

Consultation activities focused on the relevant stakeholders for **electronic identification (eID)** collected views, data and evidence on:

²¹⁵ https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

- the state of play of eID implementation in the EU and at national level under eIDAS, including any reasons hampering the notifications of eID schemes.
- types and number of services accessible and used with eIDs in the public sector including at regional and local level (e.g. eHealth, eJustice, eProcurement, eGovernment, etc.).
- number and types of private services accessible and used via the electronic identification schemes at national and cross-border level
- Actual use of eIDs schemes in public and private services, at national level and cross-border, as well as reasons hampering the adoption of eID schemes by users and providers of digital services
- Legal, conceptual, technical and policy aspects associated with the introduction of a European Digital Identity Scheme including governance of the system; the nature of the eID means; liability issues and interoperability architecture.

Consultation activities focused on the relevant stakeholders for **trust services** collected views, data and evidence on:

- number and development of trust service providers (including both qualified and non-qualified) and trust services available at national and cross border level;
- utilisation rates of trust services nationally and cross border to access public services at local, regional and national level of public administration;
- utilisation rates of trust services in different economic sectors (e.g. banking, professional services firms, etc.) and specifically the development and use of sector-specific trust services; giving particular consideration to eBanking, eCommerce, transport, login to websites and safer internet services.
- reasons hampering the adoption of eID schemes by users and providers of digital services.

3. Consultation activities

Stakeholder interviews

The evaluation was first built on a series of **14 strategic interviews** with individuals and organisations that provided strategic input in order to better define the data collection strategy and questionnaires. It helped the external contractor to fully understand the political context and current state of play regarding eID and trust services in Europe as a starting point.

Building on that, **27 targeted interviews** with different types of stakeholder helped to investigate the issues identified through desk research and strategic interviews in further detail and more targeted manner. This activity resulted in gathering more detailed information and data, in particular for the purpose of the CBA, related to the evaluation criteria and underlying evaluation questions. The interviewees were identified by the Commission during the inception phase and later adjusted in order to ensure a balanced approach.

Table 13 Overview of targeted organisations and number of interviews completed

Stakeholder type	Stakeholder outreach	No. of completed interviews
National authorities and eIDAS node operators	7 organisations	6
AB, SB, CAB	6 organisations	6

eID provider	6 organisations	5
Service provider	11 organisations	3
Q and non-Q TSP	25 organisations	7
Total targeted interviews	55 stakeholders contacted	27
Total strategic interviews	14 stakeholders contacted	14
Total interviews	69 stakeholders contacted	41

The outcome of the interviews has been integrated directly in the answers to the evaluation questions under Section 5.

Open Public consultation

The OPC was open to all stakeholders for a duration of 10 weeks until 2 October 2020. 318 respondents expressed their views on the scope, priorities and added value for the eIDAS evaluation. The questions were general, focussing on the opinion of the different stakeholders, drivers and barriers to the development and uptake of eID and trust services in Europe.

The OPC questionnaire was divided up into six sections. The first section gave respondents an introduction into the eIDAS Regulation and the evaluation study into which the OPC results would feed. The second section was made up of general profiling questions for respondents. In the third section, respondents were asked general questions related to the availability and usage of eID across borders. In the fourth section, respondents were asked general questions related to the availability and usage of trust services in Europe. The fifth section was optional and included more specific questions about rules on eID under the eIDAS Regulation and the future of digital identity. Likewise, the sixth section was optional and included more specific questions about trust services under the eIDAS Regulation. At the end of the OPC questionnaire, respondents were able to upload a document or position paper with additional information or statements related to the evaluation of the eIDAS Regulation.

Surveys

To gather primary data and fill in data gaps identified by desk research, six surveys on the EU survey platform, targeting key stakeholders were launched.

The following surveys were launched:

- **National policymakers** – Member State Representatives, in their capacity as Cooperation Network Members, Expert Group Members and/or Node Operators on the functioning of the Regulation and the costs of its implementation
- **Service providers** – public and private service providers on the functioning of the Regulation and its impact on the services they provide
- **Supervisory Bodies, Conformity Assessment Bodies, Accreditation Bodies** – responsible for the supervision of trust services
- **Trust services providers** and representation organisations of trust service
- **Identity providers** and representation organisations of identity providers
- **Technology providers**, providers of trust services not covered by eIDAS, interest representation organisations of technology providers, standardisation organisations, and other experts

Table 14 Overview of targeted organisations and number of surveys completed

Stakeholder type	Stakeholder outreach	Surveys completed	Position papers received
National authorities and eIDAS node operators	234	19	7

Service providers	91	4	1
SB, CAB, AB	126	34	6
Identity providers	85	4	0
Trust service providers	206	36	7
Technology providers, standardisation organisations, experts	62	9	5
Total	804 organisations contacted	106 surveys completed	26 position papers received

In total, 804 stakeholders were targeted. Different information needs were required per each stakeholder group and thus we have carefully tailored the surveys to the respective target group. The dissemination strategy involved a diversity of channels used for dissemination, timely communication on the survey and its purpose, limited and clear requests to stakeholders and daily monitoring of responses.

Workshops

In January 2020, a **workshop** was organized with Members of the Cooperation Network. The main purpose of this workshop was to gather additional input from Member States on the implementation of the eIDAS Regulation and state of play, including issues and opinions on the eIDAS framework.

4. Results of the Open Public Consultation

Profile of respondents

The OPC received a total of 318 replies from stakeholders. 36% of respondents indicated that they gave their contribution as an EU citizen, 31% as a company/business organisation, 11% as a business association, 9% as a public authority, 3% as an academic/research institution, 3% as an NGO, 2% as a non-EU-citizen, 0.6% as a consumer organisation and 0.1% as an environmental organisation. 23% of respondents indicated that they replied as a large organisation, 14% as a medium organisation, 10% as a small organisation, and 14% as a micro organisation. In terms of country of origin, 90% of respondents were from an EU Member State, whereas 10% of respondents came from outside of the EU, mostly from the US, the UK, Norway and Switzerland.

273 respondents answered the additional, **more specific questions** to the OPC in the area of **eID**. 74 respondents indicated that they answered to the OPC as end-users of eID (e.g. citizen, company), 57 respondents as providers of Identity and Authentication solutions and / or technologies and IT solutions in this area (e.g. software, hardware, services), 47 respondents as trade/business/professional associations or other interest representation organisations, 29 respondents as think tanks, research, academic institutions or individual experts, 23 respondents as providers of online services (private sector), 10 respondents as providers of online services (public sector), 9 respondents as public policy makers, and 8 respondents as NGOs.

217 respondents answered the additional, **more specific questions** to the OPC in the area of **trust services**. More specifically, eSignatures were of relevance to 202 respondents, eTimestamps to 145 respondents, website authentication to 144 respondents, eSeals to 139 respondents, and ERDS to 104 respondents. 61 respondents indicated that they answered to the OPC as users of electronic trust services (e.g. citizen, company, public or private service provider), 41 respondents as trade/business/professional associations or other interest representation organisations, 34 respondents as providers of electronic trust services, 31 respondents as suppliers of technologies and IT solutions for electronic trust services (e.g. software, hardware, services), 21 respondents as think tanks, research, academic institutions

or individual experts, 7 respondents as public policy makers, 4 respondents as SBs, 4 respondents as NGOs and 2 respondents as CABs.

✓ **Importance of eID and trust services during the COVID-19 crisis**

59% of respondents have found the availability of the eID means or the electronic trust services (e.g. electronic signature) **particularly useful** during the lockdown measures introduced due to the COVID-19 crisis. Out of these:

- 51% have used their eID or trust services for eGovernment services.
- 31% have used their eID or trust services for eHealth services.
- 39% have used their eID or trust services for financial services.
- 17% have used their eID or trust services for COVID-19 specific online services (e.g. reporting symptoms, test results, requesting benefits/allowance).
- 39% have used their eID or trust services for concluding contracts remotely.
- 39% have used their eID or trust services for online shopping.
- 10% indicated that they have used their eID or trust services for other services, such as conferencing apps, job applications, business contracts, organisation-internal services, insurance services.

Out of the respondents who have **not** found the availability of the eID means or the electronic trust services (e.g. electronic signature) **particularly useful** during the lockdown measures introduced due to the COVID-19 crisis:

- 26 indicated that the online services are not available for their eID / eSignature.
- 11 indicated that they could not access the online services due to usability / technical issues (e.g. lack of a card reader, software incompatibility, accessibility barriers for persons with disabilities).
- 6 indicated that they do not have them or could not get one (e.g. face to face interaction was needed to obtain/activate/renew an eID/eSignature certificate during the lockdown).
- 3 indicated a lack of trust.
- 21 indicated that they had other reasons, such as no need for it, no availability of an eID, legal inadmissibility, lack of acceptance.

64% of respondents agree that the **eIDAS Regulation** in general needs to be strengthened as a response to the COVID-19 crisis; 69% for **cross-border eID**, 77% the availability of **eSignature**, 70% the availability of **eSeal**, 66% the availability of **eTimestamp**, 68% the availability of **ERDS**, 54% the availability of **website authentication**.

✓ **eID specific questions**

Use

75% of respondents claimed that they have an electronic identification means (eID) which can be used to access online services. 59% use an eID provided by their government or other public authority, 34% have Personal user accounts provided by social networks or online platforms, and 45% own eIDs provided by other private sector organisations (e.g. trust service providers, banks, mobile operators). 51% of respondents use their eID to access or use online services at least once a week and 60% at least once per month, while 10% indicated that they use their eID to access or use online services less than once a month or never. 81% of respondents are aware that they can use one of the notified national eID schemes to access online public services in other EU Member States. 14% indicated that they have used it to access online services in another EU Member State than their country of residence, 56% have not done so yet. 63% of respondents stated that the ability to use their

eID to access public services in other EU Member States is very important or somewhat important to them.

Control of personal data

88% of respondents stated that it is very important or somewhat important for them to have a secure single digital ID that could serve for all online services (both public and private) that provides them with the control over the use of their personal data.

Mobile eID

90% of respondents stated that the ability to use their eID on their mobile phone is very important or somewhat important for them.

Availability of eID and services

In terms of services usable or potentially usable with an eID:

- 60% of respondents use their eID for public services (e.g. fill in tax form, request certificates) and 9% would like to do so.
- 23% of respondents use their eID for utility services (energy, water supply), telecom services and 38% would like to do so
- 35% of respondents use their eID for medical services (eHealth) and 29% would like to do so.
- 22% of respondents use their eID to open a bank account and 39% would like to do so.
- 20% of respondents use their eID to shop online and 29% would like to do so.
- 21% of respondents use their eID to access online platforms (e.g. social networks, online streaming accounts) and 27% would like to do so.
- 15% of respondents use their eID for other services and 18% would like to do so.

At the same time, respondents were divided on whether the number of online public services to be accessed in a cross-border context by using one of the published national eID schemes has considerably increased due to eIDAS.

Legal framework

At 55%, the majority of respondents agreed that the eIDAS Regulation provides an adequate legal framework for cross-border eID in Europe.

Interoperability

More respondents disagreed (43%) than agreed (24%) that the interoperability framework established by the eIDAS is optimal and supports sufficiently the mutual recognition of the eID schemes.

Benefits

When asked about the benefits of the use of eID to access online public services across borders, respondents widely agreed that it contributes to:

- Saving time (77% of respondents);
- The simplification of the administrative procedure (74% of respondents);
- An increase of the certainty on the authenticity of the users' identity (73% of respondents);
- The better access to services in another EU country (72% of respondents);
- Saving money (68% of respondents);
- An increase of service security (66% of respondents);
- An increase of service quality (65% of respondents);

- Enhancing user friendliness (64% of respondents);
- The access to services to a larger group of users thanks to the uptake of eID (62% of respondents);
- The protection of personal data (54% of respondents);
- Enhancing clarity on the liability of the provider of the electronic identity (51% of respondents).

Limiting factors

Despite the visible benefits, 74% of respondents stated and only 5% denied that there are currently factors limiting the cross-border use of eID. Among the factors mentioned are:

- Lack of awareness (50% of respondents);
- Limited number of notified eID schemes (50% of respondents);
- Lack of availability of relevant public services (47% of respondents);
- Limited scope of eID schemes notified under the eIDAS Regulation (governmentally issued/recognised eIDs only) (43% of respondents);
- Legal obstacles (example: face-to-face interaction required by national legislation) (40% of respondents);
- Too complicated/ not user-friendly/ accessibility barriers for persons with disabilities (36% of respondents);
- Suboptimal interoperability framework (34% of respondents);
- Lack of trust (24% of respondents);
- Privacy concerns (19% of respondents);
- Preference for paper-based solutions or face-to-face interactions (19% of respondents);
- No need for it / Not relevant (8% of respondents);
- Too expensive (6% of respondents);
- Other factors (19% of respondents). Among these factors are: lack of testability, existence of legacy systems and standards in public and private sector built for local eIDs in MSs, lack of both preparedness and legal design of end user applications to accept notified eID schemes, little involvement of the private sector and possibility for private-sector eIDs to directly notify, lack of eIDAS nodes for private-sector organisations and lack of cross-border uptake of eIDs in private sector, much market fragmentation and derogating national rules for individual applications, Cloud platform's lack of transparency, no adoption of interoperability framework by e-service providers due to high costs, lack of possibility to link digital identities and to add attributes, lack of a centralized verification mechanism for the signature providers, lack of access for people without bank account, little availability of sectorial data for specific processes, problem of identity matching between eIDAS and national IDs, incompatibility of unique identifiers and identifier schemes, lack of harmonized requirement set to be fulfilled by eID schemes in order to become notified in different MSs, low level of interaction of common citizens with public administrations abroad especially compared to their level of interaction with private-sector organisations, need for additional identity properties/attributes, lack of full interoperability across MSs due to customized data fields and solutions, poor eID software, implementation delays and inadequate preparation and compliance by MSs, existence of few use cases, lack of actual acceptance of eID schemes across borders, lack of possibility to make use of bank ID, big responsibility put on the service provider under the current framework, lack of clarity in the adequation between LOA.

Conclusions and recommendations

Overall, 40% of respondents agree and 25% disagree that the eIDAS Regulation has achieved its objectives with regard to eID. A vast majority of respondents agreed that the scope of the eIDAS Regulation should be extended to provide a level playing field for the private economic actors operating in the field of eID.

76% of respondents believe and only 1% does not believe that the **eIDAS Regulation or its implementation should be improved**. Among the **suggested corrective actions** are:

- 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 (54% of respondents);
- An obligation for Member States to make authentication available to the private sector (52% of respondents);
- 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 (50% of respondents);
- Introduction of new private sector digital identity trust services for identification, authentication and provision of attributes (47% of respondents);
- Adopting guidelines to improve legal coherence and consistency (46% of respondents);
- 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 (44% of respondents);
- A shift from voluntary to mandatory notification of national eID schemes (37% of respondents);
- Provision of identification for non-human entities (e.g AI agents, IoT devices) (33% of respondents).

51% of respondents affirmed and 21% denied that there should be 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. The following possible **advantages** of such single and uniform European digital identity scheme were flagged as important:

- Universal Acceptance (47% of respondents);
- User convenience (43% of respondents);
- Trust (Government Sponsored) (37% of respondents);
- Increased online security (32% of respondents);
- Better control of personal data (29% of respondents);
- Cost savings thanks to economies of scale (28% of respondents);
- Other advantages (8% of respondents). Among these advantages are: Accessibility and openness, Access for every European citizen regardless of income or the existence of a bank account, would fit a gap if accessible to non-EU foreigners, Avoidance of regulatory arbitrage, Basis for multi-/cross-industry use cases, Fostering Digital Europe, Settling on a limited number of implementations, Enforcement of International law cases, more harmonization across eID schemes, can serve as a fallback solution in countries in which there are not yet any notified eIDs, would achieve higher acceptance than today's notified eID schemes, can help in better separating the tasks of a public authority of checking/ascertaining the identity and attributes of a person from the task of operating technical infrastructure, Standards and coherence, decreasing effort for interoperability and integration of

further identity properties (Verifiable Credentials etc.), higher acceptance by worldwide technology companies to integrate EU eID schemes in their systems, platforms or mobile devices, simplification & comparability of LoA-assessment, higher flexibility to adapt technological developments

The following possible **disadvantages of a single and uniform European digital identity scheme** were flagged as concerning:

- Complexity of set-up and Governance (57% of respondents)
- Lack of flexibility to adapt to technological developments and changing user needs (48% of respondents)
- Overlap with existing solutions (49% of respondents)
- Discouragement of innovation and investments into alternative eID solutions (42% of respondents)
- State surveillance concerns (37% of respondents)
- Set up and operational costs (33% of respondents)

Other disadvantages (20% of respondents). Among these disadvantages are: Reliability concerns, political non-viability, undermined digital Trust in all cross-border eIDs, poor user experience, security concerns, complex implementation and interfaces, personal data storage and protection concerns, lack of technical solutions in the public sector, high costs and time, security risks, limitation of innovation, not as effective as involvement of private sector.

✓ **Trust services specific questions**

Availability

72% of respondents believe that the eIDAS Regulation has increased the availability of electronic trust services in the EU. A majority of respondents also believes that the eIDAS Regulation has increased the availability of eSignature (78% of respondents), eSeal (78% of respondents), and eTimestamp (73% of respondents). More respondents further agreed than disagreed that the eIDAS Regulation has increased the availability of ERDS (51% of respondents) and website authentication (41% of respondents), however, there was some level of disagreement with regard to these two types of trust services. Overall, only 23% of respondents agree but a majority of 54% disagree that the availability and offer of trust services in the EU is sufficient.

Usage

77% of respondents stated that they have already used electronic trust services. 65% stated that they feel more comfortable and confident to use trust services now compared to five years ago. 89% of respondents agreed that public administrations should roll out more public services, making better use of electronic trust services in their contact with citizens and businesses. A majority of respondents agreed that the use of eSignature (77% of respondents), eSeal (69% of respondents), eTimestamp (65% of respondents), ERDS (48% of respondents) and website authentication (53% of respondents) have increased in Europe during the last 3 years.

Legal effect

76% of respondents believe that providing the same legal effect to electronic trust services (e.g. qualified e-signature is equivalent to handwritten one) helped increase their take-up. 67% of respondents further agree that the legal effect provided to trust services by the eIDAS Regulation helped increase their admissibility in legal proceedings. 55% of respondents further agreed that the cross-border legal effect provided to trust services by the eIDAS Regulation helped increase their take-up.

Regarding electronic documents, 70% of respondents agree that the legal effect provided to them by the eIDAS Regulation helped increase their take-up and admissibility in legal proceedings.

Governance

Respondents were divided on the effectiveness of the governance framework provided for trust services by the eIDAS Regulation. 37% of respondents agreed and 32% disagreed that the level and scope of governance and supervision of electronic trust services are adequate to ensure harmonisation at EU level. More specifically, 42% of respondents agreed and 20% disagreed that the assessment procedure for becoming a QTSP is adequate.

Trust and confidence

A vast majority of respondents believes that the provisions of the eIDAS Regulation on trust services have enhanced trust in electronic transactions.

Technological neutrality

36% of respondents agreed and 23% disagreed that the eIDAS Regulation has put in place conditions conducive to trust services based on decentralised solutions. Despite some disagreement, a vast majority of respondents agrees that the eIDAS Regulation does not hinder technological developments in the eSignature (60% of respondents), eSeal (64% of respondents), eTimestamp (72% of respondents), ERDS (50% of respondents) and website authentication (50% of respondents) markets.

Level playing field

A majority of respondents agreed that the eIDAS regulatory framework creates a level playing field in Europe for eSignature (62% of respondents), eSeal (61% of respondents) and eTimestamp (64% of respondents). More respondents further agree than disagree that the eIDAS regulatory framework creates a level playing field for ERDS (45% of respondents) and website authentication (40% of respondents), however there is a certain level of disagreement.

Interoperability

A majority of respondents agreed that the eIDAS Regulation has ensured interoperability of eSignature (57% of respondents), eSeal (52% of respondents) and eTimestamp (59% of respondents). Opinions are more divided regarding website authentication, where 34% of respondents agreed and 26% of respondents disagreed that the eIDAS Regulation has ensured interoperability. For ERDS, more respondents disagreed (32%) than agreed (31%) that the eIDAS Regulation has ensured interoperability.

Benefits

A vast majority of respondents agreed that citizens, businesses and public administrations in Europe can effectively benefit from the advantages of eSignature (85% of respondents), eSeal (81% of respondents), eTimestamp (81% of respondents), ERDS (62% of respondents) and website authentication (65% of respondents). When asked about the following potential benefits established by the eIDAS Regulation, respondents agreed that the use of trust services contributes to:

- Saving time (85% of respondents)
- Ensuring legal certainty (84% of respondents)
- The simplification of the administrative procedure (77% of respondents)
- An increase of service security (77% of respondents)
- Saving money (72% of respondents)
- An increase of service quality (69% of respondents)

- The protection of personal data (62% of respondents)
- Enhancing user friendliness (61% of respondents)

Limiting factors

When asked about factors potentially limiting the use of electronic trust services, factors mentioned by respondents include:

- Lack of awareness (50% of respondents)
- Lack of availability for relevant services (39% of respondents)
- Too complicated/ not user-friendly/ accessibility barriers for persons with disabilities (36% of respondents)
- Preference for paper-based solutions or face-to-face interactions (24% of respondents)
- Lack of trust or fraud concerns (23% of respondents)
- Privacy concerns (19% of respondents)
- Not enough legal certainty (17% of respondents)
- Too expensive (10% of respondents)
- No need for it / Not relevant (3% of respondents)
- Other factors (15% of respondents). These include: lack of harmonisation; lack of "equivalence" defined for eSeals or ERDS; QWAC inclusion controversial; in certain EU Member States lack of QTSPs for issuing qualified certificates; difficulties on enrolment; complicated usage of QSCDs; no direct integration of QSCDs with web browsers/web signing; proof of key pair generation/operation for HSM-as-QSCD on premises of customers for QSeal doing mass signing; lack of eID availability to the private sector; missing market education; lack of acceptance of (qualified) signed electronic documents by public authorities as the default throughout the EU; lack of will among government and service providers to adapt to eIDAS; preference in many countries for use of national trust services creating additional burdens to foreign QTSPs; additional devices such as card readers required; services are not sufficiently harmonized from functional and technological perspective; no comparable level of trust and security nor EU wide interoperability; use of electronic trust services is often not visible or hard to verify for relying parties; lack of general requirement for all software publishers to verify, honour and show digital identities and signatures verified in accordance with eIDAS; lack of national legislation and guidelines on certain aspects such as remote identification methods; dependence on paper-based procedures prior to the issuance of an eSignature; legal certainty for cross-border use is limiting many use cases; EU Trusted List system only partially works and has hampered uptake of trust services; validation issue as different signing solutions produce different formats and results; multi-interpretation of the eIDAS Regulation by SBs and CABs; personal data necessary for identification are not in all cases connected to eID; no technical compatibility between services using timestamps and seals; Implementing acts setting baseline requirements for interoperability have been published only for electronic signature and seal formats; technical standards are high and expensive to implement which makes them difficult to comply with especially for smaller businesses; qualification process is not always transparent; privacy concerns related to when a document is e-signed: once biometric data is hacked it is for life; lack of promotion of the eIDAS Regulation by Member States; Lack of recognition of QWACs by major Browsers; lack of trust or fraud concerns; high costs.

Conclusions and recommendations

64% of respondents agree and 12% disagree that the eIDAS Regulation has achieved its objectives with regard to electronic trust services. Almost all respondents agree that the eIDAS Regulation is a more effective tool to regulate trust services than actions taken at national level. There is also strong and wide agreement among all stakeholder groups that repealing the eIDAS Regulation would have negative consequences for trust services in Europe. 45% of respondents stated that additional trust services should be regulated at EU level, 16% opposed this.

Respondents mentioned that the following additional trust services should be regulated at EU level:

- Electronic identification and authentication (53% of respondents)
- Provision of trusted attributes (uniquely linked to a verified identity – e.g. proof of age, credentials – professional qualifications, entitlements – Know-Your-Customer) (48% of respondents)
- Delegated management of signature keys (33% of respondents)
- eArchiving (31% of respondents)
- Operation of distributed ledgers storing electronic evidences (28% of respondents)
- Operation of identity hubs storing personal data of behalf of the users (28% of respondents)
- Other (10% of respondents)

Other suggested additional services included S/MIME, digital validation, identity validation, server signing, remote signing, one secure service for multiple purposes, Blockchain, legally irrevocable identity, eID and corporate ID, e-archiving, Attribute certificates, SIS services, identity schemes as a trust service, biometric eSignature, a single eID usable for all services, Trusted Third Party, eID issued by public and financial services, Video identification, mobile (on-)device signing, Encryption (data confidentiality) certificates to be used for e-democracy processes, Electronic voting, identity-based encryption, DID standard based identification, Authorisation services and business representation, Verifiable Credentials (VCs), eInvoicing, eTaxing, notary services, Signature verification services, Certificates for e-mail encryption, a new qualified trust service for Single Sign On (SSO), Login Services, and Tokens for Authentication.

ANNEX 3: METHODS USED IN PREPARING THE EVALUATION

This annex provides the overall evaluation framework as presented in Annex E of the external support study²¹⁶ for the evaluation. It links with the various methodological tools used (i.e. interviews, workshops, survey, open public consultation, literature review) and supplements section 4 to this report.

Electronic identification

Evaluation Question	Judgment criteria	Issues/ indicators to be analysed
Criterion: Effectiveness		
To what extent has the Regulation met its operational objectives?	The Regulation has ensured mutual recognition and acceptance of notified eIDs	<ul style="list-style-type: none"> • Availability of the eIDAS nodes • Availability of cross-border authentication on service providers website
	The Regulation has ensured interoperability of eID (cross-border and cross-sector)	<ul style="list-style-type: none"> • Governance model • Barriers to interoperability (technical, organisational...)
	The Regulation has ensured usage of notified eID by public and private sectors	<ul style="list-style-type: none"> • Number of cross border authentications • Level of usage of eID by public and private relying parties services
	The Regulation has ensured maximum reduction of administrative burden and increase of quality of services	<ul style="list-style-type: none"> • Decrease in processing time per public service using eID • Decrease in time, paperwork and hassle costs for public services using eID • Decrease in time to complete business actions using eID compared to paper alternatives increase in quality of services using eID
	The Regulation has ensured trust and confidence in the legal certainty and security of eID	<ul style="list-style-type: none"> • Stakeholder views on legal certainty & security coherence assessment

²¹⁶ Study SMART 2019/0046 evaluating the European Regulation 910/2014 (eIDAS Regulation) has been commissioned by the European Commission Directorate-General for Communications Networks, Content and Technology H4 (DG CNECT H4) and performed by Deloitte , VVA, Spark and ECORYS

To what extent has the Regulation met its specific objectives?	The Regulation has increased the availability and take-up of cross-border and cross-sector eID schemes	<ul style="list-style-type: none"> • Number of eID schemes available cross-border before the Regulation and now • Number of domestic users of eID schemes in the EU Member States before the Regulation and now
	The Regulation has stimulated the take up of cross-border electronic transactions in all sectors (public and private);	<ul style="list-style-type: none"> • Number and type of public services available for use by nationals/businesses of other MSs (G2C, G2B or G2G) • Nature and quality of incentives introduced for the public and private sector to reuse notified eIDs
	Ensure an optimal level and scope of governance	<ul style="list-style-type: none"> • Stakeholder view on the governance
	Ensure that competitive market developments are stimulated and that technological developments are not hindered in the market	<ul style="list-style-type: none"> • Evidence (e.g. studies, stakeholder perception) that the Regulation has not hindered technological development in any way
	Strengthen the competitiveness of the European industry and services sector	<ul style="list-style-type: none"> • International comparison of EU companies competitiveness
	Ensure that all consumers can benefit from the advantages of (cross-border) eID services	<ul style="list-style-type: none"> • % of citizens that are eligible to apply for a notified eID scheme • Number and type of public services available online for use by nationals or residents of another EU Member State before the Regulation and now (G2C) e.g. in (not exhaustive): taxation; requesting/delivering official documentation; residency/relocation services • Level of usage of online public services by nationals or residents of another EU Member State before the Regulation and now
To what extent has the Regulation met its general objectives?	The development of a Digital Single Market	<ul style="list-style-type: none"> • Increase in online services since 2014 is due to the Regulation
	Stimulating and strengthening sustainable competition in the Digital Single Market	<ul style="list-style-type: none"> • Market distortions or impact on competition
	To promote the interest of consumers and to ensure high level of consumer protection for all EU citizens and businesses.	<ul style="list-style-type: none"> • Stakeholder views on consumer protection
Where expectations have not been met, which factors have hindered their achievement?	[No judgement criteria needed as this section is descriptive]	<ul style="list-style-type: none"> • Horizontal analysis across all questions on the factors affecting the achievement of objectives including e.g.: <ul style="list-style-type: none"> - External factors - Legal barriers - Operation or technological barriers

		<ul style="list-style-type: none"> - Levels of awareness - Trust and security concerns - Non-availability or accessibility of services - Lack of information - Etc.
Criterion: Efficiency		
<p>Did the regulatory intervention create any additional costs and benefits for the target stakeholders?</p>	<p>Identification of costs and benefits generated by the Regulation</p>	<p>Costs:</p> <p><u>MS authorities and node operators</u></p> <ul style="list-style-type: none"> • Number of full-time employees • Annual administrative costs • Initial and recurring technical costs <p><u>Identity providers</u></p> <ul style="list-style-type: none"> • Number of full-time employees • Annual administrative costs • Initial and recurring technical costs <p><u>Service providers</u></p> <ul style="list-style-type: none"> • Number of full-time employees • Annual administrative costs <p>Initial and recurring technical costs</p> <p>Benefits:</p> <p><u>MS authorities and node operators</u></p> <ul style="list-style-type: none"> • Administrative burden reduction due to common framework • Other <p><u>Identity providers</u></p> <ul style="list-style-type: none"> • Increased market base • Other <p><u>Service providers</u></p>

		<ul style="list-style-type: none"> • Increased market base • Administrative burden reduction linked to: <ul style="list-style-type: none"> ○ Digitalisation of procedures ○ Possibility to identify remotely ○ Reduced control to verify data ○ Reduced security risks
How proportionate is the amount of costs and benefits to cost and benefit items? How are they broken down? How do they compare across different stakeholder groups?	The costs associated with the intervention are proportionate to the benefits it has generated	Quantification and comparison of: <ul style="list-style-type: none"> • Recurring administrative costs • Recurring technical costs • Initial costs • Benefits
To what extent have the aggregate costs of the Regulation have been justified and proportionate given the aggregate benefits that were achieved?	The costs borne by the stakeholders were affordable and justified	Quantification and comparison of market-aggregate costs and benefits
Are there opportunities to simplify the legislation or reduce unnecessary regulatory costs without undermining the intended objectives of the intervention?	<p>The legislation cannot be simplified and does not cause unnecessary regulatory costs</p> <p>The objectives of the Regulation could not have been achieved at a lower cost</p>	Identification of policy space for net-cost reductions
Criterion: Relevance		
To what extent do the initial objectives still correspond to current needs and concerns? In particular, how do they address concerns about data protection and security of some of the eIDs widely used by citizens (e.g. login with social networks/online platform accounts: e.g. Facebook, LinkedIn, Google)?	The original objectives are aligned with the current needs	• Original needs and objectives
		• Current consumer needs
	The original objectives are aligned with the concerns about data protection and security	• Current business needs
		• Technological developments affecting trust services
		• Current consumer concerns
		• Current business concerns

To what extent do the solutions and standards developed in relation with the eIDAS Regulation address users' needs?	The solutions and standards related to the eIDAS Regulation are aligned with users' needs	• National and international standards developed in relation with the eIDAS Regulation
		• Take-up of these standards at national and international level
		• Current needs of standard users
To what extent are there adaptation mechanisms in place to follow technological, scientific and social developments?	The Regulation is technology neutral and Adaptation mechanisms to technological, scientific and social developments exist	• New technological innovations, trends and standards relevant for fostering interoperability, transparency and user friendliness
		• Mechanisms to follow scientific developments
		• Mechanisms to follow social developments
		• Take-up and effectiveness of these adaptation mechanisms
To what extent has sector-specific legislation supported the development of relevant (e.g. mobile) eID solutions and what other areas should be covered?	Sector-specific legislation has supported the development of relevant and tailored eID solutions in the respective sectors	• Sector-specific legislation relevant for eID services • Utilisation of eID services in different economic sectors
	eID solutions are relevant for other areas and sectors	• Other non-covered areas and sectors that would need secure and interoperable eID
To what extent have alternative solutions been developed to address current needs, in parallel with the mechanisms and solutions foreseen by the eIDAS Regulation? What is the take-up of these alternative solutions?	Alternative solutions have been developed, in parallel with the eIDAS solutions and standards	• Development and take-up of alternative solutions than those foreseen by the eIDAS Regulation
		• Needs addressed by these alternative solutions
Does the eIDAS Regulation hamper their use or does the prevalence of these solutions hamper the acceptance and implementation of eIDAS standards in any way?	There is a relation between the take-up of these solutions and the implementation of the eIDAS Regulation and standards	• eIDAS Regulation provisions that limit the development and use of alternative solutions
		• Relation between the take-up of alternative solutions and the acceptance and implementation of eIDAS standards
In particular, how does the Regulation relate to the increasing use of online services on mobile devices, and to the development of solutions based on Distributed Ledgers / Blockchain technologies?	There is a relation between the eIDAS Regulation and the increasing use of online services on mobile devices	• Take-up of online services on mobile devices
	There is a relation between the eIDAS Regulation and the increasing use of online services on mobile devices and the development of solutions based on DLT/blockchain	• Extent of use of eID on mobile devices

How does the Regulation support the requirements for customer data portability (for the purpose of Know-Your-Customer and Customer Due Diligence requirements under the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing) and the emerging paradigm of full user control of their personal data (as in the MyData movement or the Decentralised Identity Foundation)?	The Regulation supports the requirements for customer data portability	<ul style="list-style-type: none"> Requirements for customer data portability (for KYC and due diligence requirements under AMLD4)
	The Regulation enables user control of their personal data	<ul style="list-style-type: none"> Provisions of the eIDAS Regulation supporting customer data portability eID services supporting customer data portability requirements
		<ul style="list-style-type: none"> Provision of the eIDAS Regulation enabling user control of their personal data eID solutions enabling user control of their personal data
How well adapted is the intervention to subsequent technological or scientific advances? What are the opportunities for expanding the number of trust services currently covered by the Regulation (by e.g. blockchain, eArchiving, IoT) and for extending eID services to the private sector?	There are opportunities for extending eID services to the private sector	<ul style="list-style-type: none"> Development of new technological solutions (by e.g. blockchain, eArchiving, IoT) relevant for fostering secure, interoperable and user-friendly electronic transactions
		<ul style="list-style-type: none"> Current use of eID services in the private sector (e.g. in online banking, eCommerce, transport, login to websites, safer internet services)
		<ul style="list-style-type: none"> Private sector areas that could benefit from eID services
Criterion: Coherence		
Are there overlaps or complementarities between the eIDAS Regulation and any other Community actions, which share objectives?	It is ensured that any other Community actions complement the provisions of the eIDAS Regulation, and do not give rise to overlapping requirements which may present relevant stakeholders with a lack of clarity about their rights or obligations.	<ul style="list-style-type: none"> Relevant Community actions with similar objectives
		<ul style="list-style-type: none"> Views of key stakeholders
Is there any issue of internal coherence of the eIDAS Regulation (i.e. between the various components of the eIDAS Regulation)? Which corrective action is advised?	It is ensured that the provisions of the eIDAS Regulation itself are coherent, and that there are no provisions that conflict or contradict each other or render each other impracticable.	<ul style="list-style-type: none"> Structured review of the eIDAS Regulation (including preparatory works where relevant to interpretation/understanding) to identify coherence issues
		<ul style="list-style-type: none"> Assessment of need for any corrective action
Is there any issue of internal coherence between the	It is ensured that all the Implementing Acts are	<ul style="list-style-type: none"> Structured review of Implementing Acts

various Implementing Acts? Which corrective action is advised (e.g. update and/or complement existing Implementing Acts)?	complementary and do not give rise to overlapping or contradictory requirements.	<ul style="list-style-type: none"> Assessment of need for corrective action
	It is ensured that the Implementing Acts reflect well their purpose as expressed in the various provisions of the eIDAS.	<ul style="list-style-type: none"> Structured review of Implementing Acts Assessment of need for corrective action
To what extent is the eIDAS Regulation coherent with similar initiatives at Member State or international level?	It is ensured that eIDAS Regulation is not incoherent with any initiatives identified at Member State or international level.	<ul style="list-style-type: none"> Existence of similar initiatives at national or international level. Assessment of any provisions with a similar purpose or scope to those in the eIDAS Regulation.
	It is ensured that the eIDAS Regulation is coherent with Member States' rules and regulations.	<ul style="list-style-type: none"> Existence of relevant rules and regulations at national level Assessment of coherence of relevant rules at national level with the relevant provisions of the eIDAS Regulation.
Are there coherence issues with relevant Member States' rules and regulations? Which corrective actions can be advised, e.g. adoption of secondary legislation, more guidance from the Commission and/or ENISA, including extending its role, tighter cooperation between Supervisory Bodies, more regular market analysis?	Need for corrective action	<ul style="list-style-type: none"> Assessment of need for corrective action and the type of corrective action which may be appropriate
Criterion: EU added value		
Is there additional value (at national, European and international level) resulting from the eIDAS Regulation, compared to what could be achieved with similar regulatory frameworks at national level?	It is ensured that the issues dealt with by the eIDAS Regulation could not be better achieved by regulatory action at national level. The Regulation has additional value at national, European and international level	<ul style="list-style-type: none"> Role entrusted to national authorities and supervisory bodies by the Regulation
		<ul style="list-style-type: none"> Cross-border activities enabled by the Regulation
		<ul style="list-style-type: none"> Use of cross-border eID
		<ul style="list-style-type: none"> International aspects of the Regulation
		<ul style="list-style-type: none"> National and international standards related to the Regulation
		<ul style="list-style-type: none"> Some change since the eIDAS was introduced which alters the conclusions regarding subsidiarity in recital 76.
Has the eIDAS Regulation added value / reinforced other elements of the Digital Single Market strategy and beyond,	It is ensured that the eIDAS Regulation has had a positive impact on other elements of the Digital Single Market and	<ul style="list-style-type: none"> Priorities of the Digital Single Market supported by the eIDAS Regulation
		<ul style="list-style-type: none"> Impact of eIDAS Regulation as potential enabler of the Services Directive

that is, in other sectors being transformed by digitalisation (such as transport, taxation, health, justice etc.)?	sectors affected by digitalisation	<ul style="list-style-type: none"> • Use of eID across sectors affected by digitalisation (e.g. transport, health, taxation, justice) • Assessment of impact of eIDAS Regulation in related sectors • Potential for eIDAS Regulation to facilitate take up of smart contracts across the EU • Impact of eIDAS Regulation as potential enabler of Council Decision 2010/48/EC (concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities)
To what extent do the issues addressed by the eIDAS Regulation continue to require action at EU level?	The persistence of issues addressed by the eIDAS Regulation still requires action at EU level	<ul style="list-style-type: none"> • Original needs addressed by the Regulation • Current needs addressed by the Regulation • Effectiveness of the Regulation in achieving its objectives • Need for further action at EU level to address any of the issues identified in evaluation criteria 1-4
What would be the most likely consequences of repealing the eIDAS Regulation?	It is ensured that the repeal of the eIDAS Regulation would have positive/negative consequences	<ul style="list-style-type: none"> • Situation before the entry into force of the Regulation • Mechanisms established by the Regulation • Unaddressed issues if the Regulation was repealed • Impact of alternative regulatory options (e.g. national/international)
Which recommendations can be made to improve the EU added value?	Would a given measure /action improve the EU added value of the Regulation?	<ul style="list-style-type: none"> • Potential amendments to the Regulation to improve its EU added value • Additional solutions and sectors that could be covered by the Regulation • Various options available to ameliorate the application of the eIDAS Regulation • How do they impact upon the various stakeholders, and on the principle of subsidiarity

Trust services

Evaluation Question	Judgment criteria	Issues/ indicators to be analysed
Criterion: Effectiveness		
To what extent has the Regulation met its specific objective of increasing the availability of trust services?	The Regulation has increased the availability of cross-border and cross-sector trust services.	<ul style="list-style-type: none"> • Number of eSignature service providers/solutions in the EU (available for domestic use and cross-border use) before the Regulation and now

		<ul style="list-style-type: none"> • Number of ERDS service providers/solutions in the EU (available for domestic use and cross-border use) before the Regulation and now • Number of eSeal service providers/solutions in the EU (available for domestic use and cross-border use) before the Regulation and now • Number of eTimestamp service providers/solutions in the EU (available for domestic use and cross-border use) before the Regulation and now • Number of WAC service providers/solutions in the EU (available for domestic use and cross-border use) before the Regulation and now • Reasons limiting the availability of trust services (if any)
To what extent has the Regulation met its specific objective of increasing the take-up of trust services?	The Regulation has increased the take-up of cross-border and cross-sector trust services.	<ul style="list-style-type: none"> • Number of domestic users and cross-border users of eSignature solutions before the Regulation and now • Number of domestic users and cross-border users of ERDS solutions before the Regulation and now • Number of domestic users and cross-border users of eSeal solutions before the Regulation and now • Number of domestic users and cross-border users of eTimestamp, Signature solutions before the Regulation and now • Number of domestic users and cross-border users of WAC solutions before the Regulation and now • Number and evolution of transactions based on trust services to access national and cross-border public (at local, regional, and national level of administration) and private services (notably in the online banking, eCommerce, transports, login to websites and safer internet services sectors) • Reasons limiting the take-up of trust services (usage)
To what extent has the Regulation met its specific objective of ensuring an optimal level and scope of governance and supervision of trust services?	The Regulation has ensured an optimal level and scope of governance of Trust Services in the EU, in particular, the supervision model of trust services has been effective	<ul style="list-style-type: none"> • Stakeholder perception on the appropriateness and effectiveness of the governance model put in place by the Regulation • Identification of weaknesses in the governance model for trust services
To what extent has the Regulation met its specific objective of ensuring stimulation of competitive market developments in the trust services market?	The Regulation has stimulated competitive market developments in the trust services market	<ul style="list-style-type: none"> • Reasons hampering the further development of trust services • Barriers to becoming a qualified service provider

To what extent has the Regulation met its specific objective of not hindering technological developments in the trust services market?	Technological developments in trust services have advanced since the implementation of the Regulation	<ul style="list-style-type: none"> Evidence (e.g. studies, stakeholder perception) that the Regulation has not hindered technological development of trust services in any way
To what extent has the Regulation met its specific objective of strengthening the competitiveness of the European industry and services sector?	The Regulation has strengthened the competitiveness of the industry and services sector through increased use of trust services.	<ul style="list-style-type: none"> Number of businesses using trust services in their business process (domestic and cross-border) before the Regulation and now Increase in market share of businesses using trust services since the adoption of the Regulation International comparison of EU companies competitiveness: Stakeholder perception on the use of trust services to strengthen the competitiveness of their business
To what extent has the Regulation met its specific objective of ensuring that all consumers can benefit from the advantages of trust services (social/digital inclusion)?	The Regulation has ensured that all consumers in the EU can benefit from the advantages of trust services.	<ul style="list-style-type: none"> Number of businesses using trust services in their business process (domestic and cross-border) before the Regulation and now Increase in market share of businesses using trust services since the adoption of the Regulation Stakeholder perception on the use of trust services to strengthen the competitiveness of their business Mutual recognition of Trust Services is enforced
To what extent has the Regulation met its specific objective of contributing to ensuring maximum reduction of administrative burden thanks to the use of trust services?	<p>The Regulation has reduced the administrative burden for public administrations using trust services.</p> <p>The Regulation has reduced the administrative burden for businesses using trust services.</p>	<ul style="list-style-type: none"> Decrease in processing time per public service using trust services Decrease in time required for administrative processes using trust services Decrease in time, paperwork and hassle costs for public services using trust services Decrease in time to complete business actions using trust services compared to paper-based alternatives
To what extent has the Regulation met its specific objective of contributing to ensuring an increase of quality of services thanks to the use of trust services?	The Regulation has increased the quality of services provided by public administrations	
To what extent has the Regulation met its specific objective of contributing to ensuring an increase of quality of business processes thanks to the use of trust services?	The Regulation has increased the quality of business processes provided by businesses	
Has the eIDAS Regulation increased cross-border use of public or private online services?	Since the implementation of the Regulation, there has been an increase in the cross-border use of public online	<ul style="list-style-type: none"> Number and type of public services available online for use by nationals or residents of another EU Member State before the Regulation and now (G2C) e.g. in (not

	services	<p>exhaustive): taxation; requesting/delivering official documentation; residency/relocation services</p> <ul style="list-style-type: none"> • Number and type of public services available online for use by businesses of another EU Member State before the Regulation and now (G2B) e.g. (not exhaustive): Taxation; Procurement; Requesting/delivering official documentation • Number and type of public services available online for use by other public administrations of another EU Member State before the Regulation and now (G2G) e.g. (not exhaustive): Requesting/delivering official documentation; Information sharing on residents, migrants, businesses, criminals etc. • Level of usage of online public services by nationals or residents of another EU Member State before the Regulation and now
Has the Regulation effectively fostered trust services that meet users' expectations and needs, e.g. by enabling mobile-friendly solutions? Are the trust services user-friendly?	The Regulation has fostered trust services that meet users' expectations and needs	<ul style="list-style-type: none"> • Existence of user-friendly trust service solutions on the market before and after the Regulation • Level of satisfaction of users (and potential users) with trust service solutions available on the market
To what extent has the Regulation met its operational objective of interoperability of trust services across borders?	The Regulation has increased interoperability of trust services in the EU	
To what extent has the Regulation met its operational objective of ensuring trust and confidence in the security of trust services?	The Regulation has positively impacted trust and confidence in the security of trust services	
To what extent has the Regulation met its operational objective of ensuring trust and confidence in the legal certainty of trust services?	The Regulation has positively impacted trust and confidence in the legal certainty of trust services	
Where expectations have not been met, which factors have hindered their achievement?	[No judgement criteria needed as this section is descriptive]	<ul style="list-style-type: none"> • Horizontal analysis across all questions on the factors affecting the achievement of objectives including e.g.: <ul style="list-style-type: none"> - External factors - Legal barriers - Operation or technological barriers - Levels of awareness - Trust and security concerns - Non-availability or accessibility of services - Lack of information - Etc.

Criterion: Efficiency

Did the regulatory intervention create any additional costs and benefits for the target stakeholders?

Identification of costs and benefits generated by the Regulation

Bodies (AC, CAB, SB)

- Administrative burden reduction due to common framework
- Other

Qualified trust service providers

- Reduction of legal advice costs related to cross-border operation
- Qualified status:
 - Increased security
 - Signalling effect
 - Compliance with public sector requirements (e.g. tendering)
- Reduction of administrative burden linked to
 - Digitalisation of procedures
 - Interoperability
 - Controls of authenticity
- Market benefits:
 - Added revenue
 - Increased market base

Non-qualified trust service providers

- Reduction of legal advice costs related to cross-border operation
- Reduction of administrative burden linked to
 - Digitalisation of procedures
 - Interoperability
 - Controls of authenticity
- Market benefits:
 - Added revenue
 - Increased market base

		<ul style="list-style-type: none"> • Reduction of compliance costs
How proportionate is the amount of costs and benefits to cost and benefit items? How are they broken down? How do they compare across different stakeholder groups?	The costs associated with the intervention are proportionate to the benefits it has generated	<p>Quantification and comparison of:</p> <ul style="list-style-type: none"> • Recurring administrative costs • Recurring technical costs • Initial costs • Benefits
To what extent have the aggregate costs of the Regulation have been justified and proportionate given the aggregate benefits that were achieved?	The costs borne by the stakeholders were affordable and justified	Quantification and comparison of market-aggregate costs and benefits
Are there opportunities to simplify the legislation or reduce unnecessary regulatory costs without undermining the intended objectives of the intervention?	<p>The legislation cannot be simplified and does not cause unnecessary regulatory costs</p> <p>The objectives of the Regulation could not have been achieved at a lower cost</p>	Identification of policy space for net-cost reductions
Criterion: Relevance		
To what extent do the initial objectives still correspond to current needs and concerns?	The original objectives are aligned with the current needs	<ul style="list-style-type: none"> • Original needs and objectives • Current consumer needs • Current business needs • Technological developments affecting trust services
	The original objectives are aligned with the concerns about data protection and security	<ul style="list-style-type: none"> • Current consumer concerns • Current business concerns
To what extent do the solutions and standards developed in relation with the eIDAS Regulation address users' needs?	The solutions and standards related to the eIDAS Regulation are aligned with users' needs	<ul style="list-style-type: none"> • National and international standards developed in relation with the eIDAS Regulation • Take-up of these standards at national and international level
		<ul style="list-style-type: none"> • Current needs of standard users
To what extent are there adaptation mechanisms in place to follow technological, scientific and	The Regulation is technology neutral and Adaptation mechanisms to technological, scientific and social	<ul style="list-style-type: none"> • New technological innovations, trends and standards relevant for fostering interoperability, transparency and user friendliness

social developments?	developments exist	<ul style="list-style-type: none"> • Mechanisms to follow scientific developments
		<ul style="list-style-type: none"> • Mechanisms to follow social developments
		<ul style="list-style-type: none"> • Take-up and effectiveness of these adaptation mechanisms
To what extent has sector-specific legislation supported the development of relevant (e.g. mobile) trust service solutions and what other areas should be covered?	Sector-specific legislation has supported the development of relevant and tailored trust solutions in the respective sectors	<ul style="list-style-type: none"> • Sector-specific legislation relevant for trust services • Utilisation of trust services in different economic sectors • Development and use of sector-specific trust services (especially for online banking, eCommerce, transport, login to websites, safer internet services)
	Trust service solutions are relevant for other areas and sectors	<ul style="list-style-type: none"> • Other non-covered areas and sectors that would need secure and interoperable electronic transactions
To what extent have alternative solutions been developed to address current needs, in parallel with the mechanisms and solutions foreseen by the eIDAS Regulation? What is the take-up of these alternative solutions?	Alternative solutions have been developed, in parallel with the eIDAS solutions and standards	<ul style="list-style-type: none"> • Development and take-up of alternative solutions than those foreseen by the eIDAS Regulation
		<ul style="list-style-type: none"> • Needs addressed by these alternative solutions
Does the eIDAS Regulation hamper their use or does the prevalence of these solutions hamper the acceptance and implementation of eIDAS standards in any way?	There is a relation between the take-up of these solutions and the implementation of the eIDAS Regulation and standards	<ul style="list-style-type: none"> • eIDAS Regulation provisions that limit the development and use of alternative solutions
		<ul style="list-style-type: none"> • Relation between the take-up of alternative solutions and the acceptance and implementation of eIDAS standards
In particular, how does the Regulation relate to the increasing use of online services on mobile devices, and to the development of solutions based on Distributed Ledgers / Blockchain technologies?	There is a relation between the eIDAS Regulation and the increasing use of online services on mobile devices	<ul style="list-style-type: none"> • Take-up of online services on mobile devices
	There is a relation between the eIDAS Regulation and the increasing use of online services on mobile devices and the development of solutions based on DLT/blockchain	<ul style="list-style-type: none"> • Extent of use of trust services on mobile devices • Development and take-up of trust solutions based on DLT/blockchain
How does the Regulation support the requirements for customer data portability (for the purpose of Know-Your-Customer and Customer Due Diligence requirements under the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money	The Regulation supports the requirements for customer data portability	<ul style="list-style-type: none"> • Requirements for customer data portability (for KYC and due diligence requirements under AMLD4)
		<ul style="list-style-type: none"> • Provisions of the eIDAS Regulation supporting customer data portability
		<ul style="list-style-type: none"> • Trust services supporting customer data portability requirements

laundering or terrorist financing) and the emerging paradigm of full user control of their personal data (as in the MyData movement or the Decentralised Identity Foundation)?	The Regulation enables user control of their personal data	<ul style="list-style-type: none"> • Provision of the eIDAS Regulation enabling user control of their personal data
	The Regulation enables user control of their personal data	<ul style="list-style-type: none"> • Trust service solutions enabling user control of their personal data
How well adapted is the intervention to subsequent technological or scientific advances? What are the opportunities for expanding the number of trust services currently covered by the Regulation (by e.g. blockchain, eArchiving, IoT) and for extending eID services to the private sector?	There are opportunities for expanding the number of trust services	<ul style="list-style-type: none"> • Development of new technological solutions (by e.g. blockchain, eArchiving, IoT) relevant for fostering secure, interoperable and user-friendly electronic transactions
Criterion: Coherence		
Are there overlaps or complementarities between the eIDAS Regulation and any other Community actions, which share objectives?	It is ensured that any other Community actions complement the provisions of the eIDAS Regulation, and do not give rise to overlapping requirements which may present relevant stakeholders with a lack of clarity about their rights or obligations.	<ul style="list-style-type: none"> • Relevant Community actions with similar objectives • Views of key stakeholders
Is there any issue of internal coherence of the eIDAS Regulation (i.e. between the various components of the eIDAS Regulation)? Which corrective action is advised?	It is ensured that the provisions of the eIDAS Regulation itself are coherent, and that there are no provisions that conflict or contradict each other or render each other impracticable.	<ul style="list-style-type: none"> • Structured review of the eIDAS Regulation (including travaux préparatoires where relevant to interpretation/understanding) to identify coherence issues • Assessment of need for any corrective action
Is there any issue of internal coherence between the various Implementing Acts? Which corrective action is advised (e.g. update and/or complement existing Implementing Acts)?	It is ensured that all the Implementing Acts are complementary and do not give rise to overlapping or contradictory requirements.	<ul style="list-style-type: none"> • Structured review of Implementing Acts • Assessment of need for corrective action
	It is ensured that the Implementing Acts reflect well their purpose as expressed in the various provisions of the eIDAS.	<ul style="list-style-type: none"> • Structured review of Implementing Acts • Assessment of need for corrective action

To what extent is the eIDAS Regulation coherent with similar initiatives at Member State or international level?	It is ensured that eIDAS Regulation is not incoherent with any initiatives identified at Member State or international level.	<ul style="list-style-type: none"> • Existence of similar initiatives at national or international level. • Assessment of any provisions with a similar purpose or scope to those in the eIDAS Regulation.
	It is ensured that the eIDAS Regulation is coherent with Member States' rules and regulations.	<ul style="list-style-type: none"> • Existence of relevant rules and regulations at national level • Assessment of coherence of relevant rules at national level with the relevant provisions of the eIDAS Regulation.
Are there coherence issues with relevant Member States' rules and regulations? Which corrective actions can be advised, e.g. adoption of secondary legislation, more guidance from the Commission and/or ENISA, including extending its role, tighter cooperation between Supervisory Bodies, more regular market analysis?	Need for corrective action	<ul style="list-style-type: none"> • Assessment of need for corrective action and the type of corrective action which may be appropriate
Criterion: EU added value		
Is there additional value (at national, European and international level) resulting from the eIDAS Regulation, compared to what could be achieved with similar regulatory frameworks at national level?	It is ensured that the issues dealt with by the eIDAS Regulation could not be better achieved by regulatory action at national level. The Regulation has additional value at national, European and international level	<ul style="list-style-type: none"> • Role entrusted to national authorities and supervisory bodies by the Regulation
		<ul style="list-style-type: none"> • Cross-border activities enabled by the Regulation
		<ul style="list-style-type: none"> • Use of cross-border trust services
		<ul style="list-style-type: none"> • International aspects of the Regulation
Is there additional value (at national, European and international level) resulting from the eIDAS Regulation, compared to what could be achieved with similar regulatory frameworks at national level?	It is ensured that the issues dealt with by the eIDAS Regulation could not be better achieved by regulatory action at national level. The Regulation has additional value at national, European and international level	<ul style="list-style-type: none"> • National and international standards related to the Regulation
		<ul style="list-style-type: none"> • Some change since the eIDAS was introduced which alters the conclusions regarding subsidiarity in recital 76.
Has the eIDAS Regulation added value / reinforced other elements of the Digital Single Market strategy and beyond, that is, in other sectors being transformed by digitalisation (such as transport, taxation, health, justice etc.)?	It is ensured that the eIDAS Regulation has had a positive impact on other elements of the Digital Single Market and sectors affected by digitalisation	<ul style="list-style-type: none"> • Priorities of the Digital Single Market supported by the eIDAS Regulation
		<ul style="list-style-type: none"> • Impact of eIDAS Regulation as potential enabler of the Services Directive
		<ul style="list-style-type: none"> • Use of trust services across sectors affected by digitalisation (e.g. transport, health, taxation, justice)
		<ul style="list-style-type: none"> • Assessment of impact of eIDAS Regulation in related sectors

	It is ensured that the eIDAS Regulation has had a positive impact on other elements of the Digital Single Market and sectors affected by digitalisation	<ul style="list-style-type: none"> • Potential for eIDAS Regulation to facilitate take up of smart contracts across the EU • Impact of eIDAS Regulation as potential enabler of Council Decision 2010/48/EC (concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities)
To what extent do the issues addressed by the eIDAS Regulation continue to require action at EU level?	The persistence of issues addressed by the eIDAS Regulation still requires action at EU level	<ul style="list-style-type: none"> • Original needs addressed by the Regulation • Current needs addressed by the Regulation • Effectiveness of the Regulation in achieving its objectives • Need for further action at EU level to address any of the issues identified in evaluation criteria 1-4
What would be the most likely consequences of repealing the eIDAS Regulation?	It is ensured that the repeal of the eIDAS Regulation would have positive/negative consequences	<ul style="list-style-type: none"> • Situation before the entry into force of the Regulation • Mechanisms established by the Regulation • Unaddressed issues if the Regulation was repealed • Impact of alternative regulatory options (e.g. national/international) • Impact of pure self-regulation on trust services
Which recommendations can be made to improve the EU added value?	Would a given measure /action improve the EU added value of the Regulation?	<ul style="list-style-type: none"> • Potential amendments to the Regulation to improve its EU added value • Additional solutions and sectors that could be covered by the Regulation • Various options available to ameliorate the application of the eIDAS Regulation • How do they impact upon the various stakeholders, and on the principle of subsidiarity

ANNEX 4: ADDITIONAL INFORMATION

This annex provides additional information to Section 2 of the SWD: Background - Baseline and points of comparison.

Electronic identification

As described in Section 2, a number of different factors led to a **limited use of public and private online services** before the adoption of the eIDAS Regulation.

As a response to these challenges and with the aim to **ensure mutual recognition and acceptance of notified eIDs**, Article 6 of the eIDAS Regulation introduced the principle of mutual recognition of eID means to access online public services cross-border. Article 12 and implementing act 2015/296 define cooperation arrangements between Member States to implement the mutual recognition principle, such as the process of notification²¹⁷ and joint peer reviewing of new schemes by Member States' experts.

In addition, article 12 and implementing act 2015/1501 aim to **ensure the interoperability of technically diverse national eID schemes** through a system of technical nodes and rules related to data privacy and integrity, security standards, identification data, message formats and other technical specifications.

For the use of eID in practice, online service providers need certainty that a specific eID offers the appropriate level of assurance in terms of trust, security and data protection required for the respective online service. Hence, service providers dealing with sensitive information or transactions require an eID that is highly trustworthy while this might not be necessary in less-sensitive use-cases. In order to capture this variety, the eIDAS Regulation introduced three levels of assurance – low, substantial and high – for notified eID schemes as per article 8 of the Regulation and set up minimum technical specifications and procedures each of them as per implementing act 2015/1502. For instance, a high level of assurance requires more elements related to identity proofing, verification and the authentication mechanism.

Another layer of security is added in Article 10 of the eIDAS Regulation obliging Member States to suspend and revoke cross-border authentication and to inform other Member States and the Commission without delay in case of a security breach.

While these measures intend to **ensure trust and confidence in the security** of notified eIDs, the need for **legal certainty** of notified eIDs is addressed by article 11 which determines the liability of the notifying Member State in case of damage caused due to a failure to comply with the obligations set.

By setting up a common legal and technical framework for eID, the eIDAS Regulation also aims to **reduce administrative burden and to increase the quality of cross-border public service provision in the EU**. With its objective to **strengthen competitiveness and ensure technological neutrality** in the field of eID, the eIDAS Regulation also seeks to contribute to Single Market objectives and promotes the interests and the protection of consumers.

Trust services

In the field of trust services, the challenges described in Section 2 had adverse effects on interoperability and the functioning of the Single Market.

²¹⁷ Article 7 and further defined in implementing act 2015/1984 regarding circumstances, formats and procedures.

The eIDAS Regulation seeks to address these issues through a number of key measures:

1. It provides for **non-discrimination of electronic forms** vis-à-vis the paper equivalent, requiring that electronic trust services shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds of their electronic form²¹⁸;
2. It prohibits **restrictions of trust services** provided by a trust service provider established in another Member State;
3. It creates “**qualified trust services**” (QTS)²¹⁸ and “**qualified trust service providers**” (QTSPs) which all Member States are required to recognise once the qualified status is granted by the supervisory authorities of the Member State of establishment²¹⁹.

The “qualified” level defined in the eIDAS Regulation for each type of trust service carries the presumption of reliability and mutual recognition between Member States. It ensures legal certainty, but also liability and burden of proof which are the key factors of difference to non-qualified trust service providers. QTSPs are liable for damage by intention or negligence²²⁰ and need to bear the burden of proof while for non-qualified providers, the burden of proof remains with the complainant. On the other hand, when issuing a qualified certificate, QTSPs must verify to whom the qualified certificate is issued by physical presence, remote electronic identification or other identification methods recognised at Member State level.

4. In order to create a level playing field, the eIDAS Regulation includes common rules for a **supervisory framework** which each Member State needs to establish.

The framework includes three main actors, the supervisory body, the conformity assessment body (CAB) and the national accreditation body and ensures through *ex ante* and *ex post* supervision that service providers and trust services meet the requirements. Article 18 of the Regulation provides for the principle of mutual assistance between supervisory bodies. A supervisory body shall provide assistance upon a justified request from another body to ensure an optimal level and scope of governance of European trust services.

Conformity assessment bodies (CABs)²²¹ are responsible for providing a conformity assessment report for the purposes of initiating QTSPs under Article 21 of the Regulation and conducting conformity assessments to ensure that the necessary regulatory requirements are being met. The supervision of QTSPs is governed by Article 20 of the Regulation. Under the provision, all QTSPs are to be audited at their own expense at least every 24 months by a conformity assessment body, with the central objective being to confirm that the QTSP and the QTSs it provides meet the requirements laid down in the Regulation. This provision tackles the issue of market fragmentation and lack of trust that occurred as a result from the patchwork supervision that occurred under the old framework.

²¹⁸ Article 3(17) of the Regulation – qualified trust service ‘means a trust service that meets the applicable requirements laid down in this Regulation.’

²¹⁹ The responsibility of granted a trust service provider qualified status ultimately lies with the supervisory body, in accordance with Article 21 of the Regulation

²²⁰ Pursuant to Article 13 of the eIDAS Regulation

²²¹ Compiled list of CABs as defined in Article 2(13) of the Regulation can be found here:
https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accruited_cabs-2019-11-28.pdf

All CABs must be formally accredited²²² by the Member State's appointed national accreditation body²²³, who has authority from the derived state. All CABs must be accredited 'in such a way that their accreditation ensures that they are competent to carry out the conformity assessment of a QTSP/QTS against the requirements of the eIDAS Regulation'²²⁴. Other relevant bodies in the supervisory framework include data protection authorities at national and European level (European Data Protection Supervisor) and ENISA.²²⁵

Article 22 requires each Member State to establish, maintain and publish **trusted lists**, including information related to the qualified trust service providers for which it is responsible. Both qualified and non-qualified trust service providers²²⁶ and trust services can be included on the Trusted Lists. Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 lays down technical specifications and formats to be followed relating to trusted lists,²²⁷ which 'are essential for the building of trust among market operators as they indicate the status of the service provider at the moment of supervision'²²⁸. Trusted lists contain not only the information of the current status of the trust service provider and trust service but also of its history. They are the only reliable source to validate and verify the status of a trust service provider and its trust service at any given point in time and have constitutive value.²²⁹ Following the initiation of a QTSPs, the supervisory body is obliged to notify the Commission on any changes made to the relevant Member State's Trusted List.²³⁰ ENISA has published guidelines²³¹ on the supervision of trust services.

²²² In accordance to : Article 3(18) of the eIDAS Regulation requires CABs to be formally accredited in accordance with Regulation (EC) No 765/2008

²²³ Accreditation for the certification of trust service providers under the eIDAS Regulation (2017). see: <https://www.ukas.com/news/accreditation-for-the-certification-of-trust-service-providers-under-the-eidas-regulation/>

²²⁴ <https://www.enisa.europa.eu/publications/tsp-supervision>

²²⁵ Relevant data protection authorities must be notified when a breach of data protection and/or security has occurred at the relevant level. Supervisory bodies must provide an annual report to ENISA summarising notifications of security breaches and loss of integrity received from trust service providers (Article 19(3)).

²²⁶ Article 3(20) of the Regulation – trust service providers 'means a natural or legal person who provides one or more trust services either as a qualified or non-qualified trust service provider'.

²²⁷ Commission Implementing Decision (EU) 2015/1505 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5), see here: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1505&from=EN>

²²⁸ Recital 1 of the Implementing Decision (EU) 2015/1505

²²⁹ Trust services under the eIDAS Regulation (2018). See here: <https://portail-qualite.public.lu/dam-assets/publications/confiance-numerique/trustservices-under-eIDAS.pdf>

²³⁰ In accordance to Article 22 (3) on Trusted Lists of the Regulation

²³¹ [Guidelines on Supervision of Qualified Trust Services - Technical guidelines on trust services \(ENISA, 2017\)](https://www.enisa.europa.eu/publications/tsp-supervision/at_download/fullReport), see: https://www.enisa.europa.eu/publications/tsp-supervision/at_download/fullReport