EUROPEAN
COMMISSION

Brussels, 3.6.2021
SWD(2021) 124 final

PART 1/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

Proposal for a Regulation

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

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

TABLE OF CONTENTS

TABLE OF FIGURES

GLOSSARY

Term or acronym	Meaning or definition
AI	Artificial intelligence
AML	Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing – "anti-money laundering directive"
Attributes	Pieces of information about one person or organisation. This could include details from the government – such as your legal name, date of birth, social security number— as well as details from other organisations, such as your professional qualifications, employment history, licenses etc.
Authentication	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
CAB	Conformity Assessment Body
CDD	Customer due diligence". Term used in financial services to require professionals to verify the identity, suitability and risks involved in engaging in their financial dealings.
CEF	Connecting Europe Facility. EU Funding programme supporting the development of interconnected trans-European networks in the fields of transport, energy and digital services.
CEF Building blocks	Open and reusable digital solutions: a framework, a standard, a software, or a software as a service (SaaS), or any combination thereof endorsed by the European Commission and supporting eDelivery, eSignatures and other digital trust service funded by the Connecting Europe Facility programme
Credential	Is a set of claims that prove qualification, achievement, quality or aspect of a person's background. The term credential might be used as a basic identity attribute or attestation based on digital identity.
eID	Government electronic identification. It means 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.
Digital identity means	material and/or immaterial unit containing person identification data and which is used for authentication for an online service
Digital identity solutions	Digital identification of various kind provided by the private or public sector which may include the provision of attributes and credentials
eID scheme	A system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons
eIDAS	Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market
eIDAS node	An eIDAS Node is an application component that can assume two different roles depending on the origin of a received request, as a connector when located in the Member States of the Service Providers or as a Proxy Service when located in the Member State of the citizen
ERDS	Electronic Registered Delivery Service

Term or acronym	Meaning or definition
Gatekeepers	Provider of core platform services with significant impact on the internal market, providing gateways for a large number of business users, to reach end users, everywhere in the Union and on different markets (see: COM(2020)842 final – Recital 6 and Art.2)
SE	Secure Element. Tamper resistant platform capable of securely hosting applications and storing confidential and cryptographic data. There are different forms of SE: embedded and integrated (eSE), smart cards, etc.
ETSI	European Telecommunications Standards Institute
EUCC scheme	Common Criteria based European candidate cybersecurity certification scheme
FESA	Forum of European Supervisory Authorities for trust service providers
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications
Identity provider	An entity that creates, maintains and manages identity information and provides authentication services
IoT	Internet of Things
Level of assurance (LoA)	According to ISO/IEC 29115, a LoA describes "the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity claiming a particular identity (i.e., the entity) is in fact the entity to which that identity was assigned". Under eIDAS, a notified eID scheme shall specify assurance levels low, substantial and/or high
LOTL	European List of Trusted Lists
Notified eID scheme	National eID notified by Member States for mutual recognition under eIDAS. The notification process ensures mutual recognition of the eID scheme across the EU.
OOP	Once-only principle, seeking to allow citizens and businesses to provide their data only once to public administrations
OPC	Open Public Consultation
PSD2	Directive (EU) 2015/2366 on payment services in the internal market
Qualified certificate	'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV
QTS / NQTS	Qualified Trust Service / Non-Qualified Trust Service
QTSP / NQTSP	Qualified Trust Service Provider / Non-Qualified Trust Service Provider
QWAC	Qualified Website Authentication Service – digital certificate created by the eIDAS regulation (art.45) and issued by qualified trust service providers attesting to the identity of the entity responsible for a specific website
SB	(National) Supervisory Body
SDGR	Single Digital Gateway Regulation
SOG-IS MRA	Senior Officials Group Information Systems Security - Mutual Recognition Arrangement
TSP	Trust service provider

1 INTRODUCTION

1.1 POLITICAL AND LEGAL CONTEXT

In her State of the Union address of 16 September 2020, the President of the European Commission announced the Commission's ambition to deliver a secure and trusted digital identity to all EU citizens:

> *"We want a set of rules that puts people at the centre. (...) This includes control over our personal data, which we still have far too rarely today. Every time an app or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used".*

The European Council seconded the Commission's ambition and, in the Council Conclusions of 1-2 October 2020[1], called on the Commission to come forward with a proposal for a European digital identity framework initiative by mid-2021:

> *The European Council Conclusions call for "The development of an EU-wide framework for secure public electronic identification (eID), including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services". The Council invites the Commission to come forward with a proposal for a European digital identity framework initiative by mid-2021."*

Electronic identification allows citizens and businesses to prove who they are when accessing services online. Trust services, such as electronic signatures[2], make online transactions more secure, convenient and efficient. The eIDAS Regulation[3] (eIDAS) is the only cross-border framework for trusted electronic identification (eID) of natural and legal persons, and trust services. eIDAS enables the cross-border recognition of government eIDs for access to ***public services***, under the condition the eID has been notified under eIDAS. eIDAS also establishes an EU market for trust services recognised across borders with the same legal status as their traditional equivalent paper-based processes.

How eIDAS works: The eIDAS Regulation does not harmonise national ***eIDs*** but enables their mutual recognition through a notification process. Once a Member State has notified a national eID scheme to the Commission, Member States' experts will do a peer-review of the scheme, assessing its compliance with the criteria set out in the eIDAS Regulation[4], implementing acts and guidelines[5]. Only Member States can notify[6] eID schemes and this is done on a ***voluntary*** basis. Moreover, there is currently no obligation for Member States to provide their citizens and businesses with eID enabling secure access to public services. eIDAS establishes three levels of assurance (low, substantial and high[7]), and each level has certain minimum criteria and functional requirements. Following the notification and the completion of the peer-review process, the scheme will be mutually recognised in all Member States.

For the mutual recognition to work in practice, national eID schemes need to be interoperable. As the regulation does not harmonise technical standards, an interoperability framework[8] with technical nodes ("eIDAS nodes") to which services need to connect has been established to ensure the cross-border identification of users.

---

[1] https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

[2] The trust services established under eIDAS are electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23.7.2014 on electronic identification and trust services for electronic transactions in the internal market, OJ L 257/73 of 28.8.2014.

[4] Article 9 of eIDAS lays down the notification process

[5] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework; Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification; Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification.

[6] eID schemes by private sector providers can be notified under eIDAS only if they are recognised by, or provided on behalf of a Member State

[7] Article 8 of the eIDAS regulation

[8] Article 12 of the eIDAS regulation

In addition to eID, the eIDAS regulation provides a ***legal framework for trust services***, such as electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication certificates. Unlike for eIDs, trust services do not need to go through any peer review or evaluation by other Member States to be recognised cross-border. eIDAS establishes the legal framework and market rules to ensure that trust services are provided and recognised across borders with the same legal effect in all Member States as their traditional equivalent paper-based processes. eIDAS provides the highest probative value and legal certainty only to ***qualified*** trust services (which are equivalent to the physical / paper-based ones). Qualified trust services and qualified trust service providers (as opposed to non-qualified) are subject to a strict supervision by Member States' dedicated authorities that verify whether they comply with the requirements laid down in eIDAS. Member States maintain national lists of qualified providers of trust services and of the qualified services they provide, which are communicated to and published by the Commission.

The eIDAS regulation allows natural and legal persons to safely access services and carry out transactions online across borders, and has thus become ***a fundamental element to facilitate the single market in a number of sectors.*** For example, financial services have to comply with requirements on secure customer identification. eIDs under eIDAS are able to supply some of the required identity data[9] to facilitate compliance with Anti-Money Laundering rules (AML)[10]. The Payment Services Directive (PSD2)[11] builds on eIDAS trust services, such as eSeals and Qualified Website Authentication Certificates (QWACs) to identify the authenticity of websites by third-party payment providers[12]. Secure online identification, based on eIDAS, is a requirement for the exchange of administrative certificates across borders, and is essential for the successful implementation and functioning of the Once-only principle (OOP) that will come into effect in 2023[13]. eIDAS is referenced in the Company law Directive as regards the use of digital tools and processes[14]. The eIDAS trust services framework is recognised internationally, and forms the basis for a draft provision[15], expected to become a UN model law on trust services in electronic commerce in 2021, as well as for the ongoing electronic trade negotiations within the WTO[16].

While eIDAS plays an undisputed role in the internal market, a lot has changed since its adoption. eIDAS, adopted in 2014, is based on national eID systems following diverse standards and focuses on a relatively small segment of the electronic identifications needs of citizens and businesses: secure cross-border access to ***public services***. The services targeted mainly concern the 3%[17] of EU's population residing in a Member State different from the one they were born in.

Since then, digitalisation of all functions of society has increased dramatically. Not least has the COVID-19 pandemic had a very strong effect on the speed of digitalisation. A McKinsey survey suggests that COVID-19 has accelerated digitalisation by 7 years globally[18]. 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*** such as submitting tax declarations, enrolling in a foreign university,

[9] Such as name, address, date of birth, nationality

[10] Directive (EU) 2015/849 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 (EU) No 648/2012 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

[11] Directive (EU) 2015/2366 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 (EU) No 1093/2010, and repealing Directive 2007/64/EC

[12] 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.

[13] The Once Only Principle will, from 2023, allow public administrations to reuse and share data and documents that people have already supplied in a transparent and secure way. (Article 14 of 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. OJ L 295 of 21.11.2018).

[14] Directive (EU) 2017/1132 relating to certain aspects of company law : "Member States should ensure that secure electronic identification and the use of trust services is possible for national as well as cross-border users in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council"

[15] https://undocs.org/en/A/CN.9/WG.IV/WP.167

[16] See e.g. Session documents for UNCITRAL Working Group IV / Electronic Commerce, Session 6-9 April 2021: https://uncitral.un.org/en/working_groups/4/electronic_commerce

[17] https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

[18] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#

remotely opening a bank account or asking for a loan, renting a car, setting up a business in another Member State, authenticating for internet payments, bidding to an online call for tender, and more.

As a consequence, the demand for ***means to identify and authenticate online***, as well as to digitally ***exchange information related to our identity***, attributes or qualifications (identity, addresses, age, but also professional qualifications, driving licences and other permits and payment systems), securely and with a high level of data protection, has increased radically[19].

This has triggered a ***paradigm shift***, moving towards advanced and convenient ***solutions*** that are able to integrate different verifiable data and certificates of the user. Users expect a self-determined environment where a variety of different credentials and attributes can be carried and shared such as for example your national eID, professional certificates, public transport passes or, in certain cases, even digital concert tickets[20]. These are so-called ***self-sovereign app-based wallets*** managed through the ***mobile device*** of the user allowing for a secure and easy access to different services, both public and private, under his or her full control.

Today, this demand cannot be fulfilled by the eID means and trust services as regulated by eIDAS, given its current limitations. As regards identification or authentication means, developed by the private sector outside the eIDAS framework they only partly answer to this challenge. While they offer user-friendly third-party authentication services (e.g. using a Facebook or Google account to log in to different services), they are common to access unregulated ***private online services that do not require a high level of security*****.** They cannot offer the same level of legal certainty, data protection and privacy, mainly because they are self-asserted and cannot offer a link to trusted and secure government eID. As regards the digital exchange of attributes or qualifications, public and private offer is scattered and lacks cross-border legal effects[21].

Article 49 of eIDAS requires the Commission to review the application of the regulation no later than July 2020, particularly to evaluate whether it is appropriate to modify its scope or its specific provisions taking into account technological, market and legal developments[22]. This impact assessment bases itself on the evaluation report coming out of such review[23].

In February 2020, the Commission committed itself in its ***Strategy on Shaping Europe's Digital Future***[24] to revise the eIDAS Regulation aiming to improve its effectiveness, extend its application to the private sector and promote trusted digital identities for all EU citizens and businesses. The urgency of this revision became clear with the outbreak of the COVID-19 pandemic. The disruptions to offline public and private services, and the sudden need for accessing and using all types of public and private services online, revealed the failure of eIDAS in delivering the expected benefits to citizens, businesses and governments six years from its adoption. As a consequence, a majority of respondents to an Open Public Consultation[25] agreed that eIDAS should be strengthened[26].

A revised and strengthened eIDAS Regulation would be able to answer to new market and societal demands by addressing the needs for trusted government eIDs linked solutions, but also for attributes and credentials provided by the public and private sector, all being fully managed by the user and recognised across the EU to access both public and private services. This would support a large number of existing or proposed regulatory frameworks strengthening the EU's Single Market such as the ongoing strengthening of the EU

---

[19] For instance, in Italy the number of users of SPID (launched in 2016) at the end of 2019 was ~5 million. Today, the active users are more than 18 million active (see https://avanzamentodigitale.italia.it/it/progetto/spid) with a steadily increase of ~1 million users per month. The use of SPID went from ~55 million for the entire year 2019 to ~32,4 in the sole month of February 2021

[20] Emerging public sector developed ID wallet, such as the German Optimos2 project, pursue a similar 'mixed approach' combining secure credentials with simple online passes and tickets for daily use.

[21] See Section 2.

[22] "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."

[23] See eIDAS Evaluation SWD (2021)

[24] European Commission. (2020). Strategy on Shaping Europe's Digital Future Strategy on Shaping Europe's Digital Future

[25] Open Public Consultation for the Evaluation of eIDAS was open for contributions 24 July – 2 October 2020

[26] Specific results: Support to strengthening of the eIDAS legal framework for cross-border eID (69% of respondents), the availability of eSignature (77% of respondents), eSeals (70% of respondents), eTimestamps (66% of respondents), ERDS (68% of respondents) and website authentication (54% of respondents).

anti-money laundering framework[27], a future European digital driving license, a future European Social Security Passport, the Digital Euro[28], a European Maritime Single Window environment[29], the Regulation on Electronic Freight Transport Information [30] or the initiative for developing an EU Single Window environment for customs[31].

The COVID-19 pandemic also highlighted the potential of digital identity to support the recovery and resilience of the European economy. Smart investments in digital technologies, among them eID and trust services, are one of the pillars for the EU Recovery Plan[32]. A stronger and wider European framework for the provision of trusted electronic identity solutions underpinned by legal identities provided by Member States can boost global trade and support competitive advantage of the EU-based enterprises. This can foster the competitive advantage of European businesses globally, through greater digitalisation (and thus, efficiency and effectiveness) of their service offering. Moreover, it can also trigger the development of new cross-borders markets related to identity, such as the one for the provision and exchange of attributes related to identity, (e.g. name, address and age, medical certificates or other types of information linked to a person such as a professional qualifications or a digital driver's licence).

Building on the evaluation of the eIDAS regulation, this impact assessment explores the challenges and the problem drivers preventing citizens and businesses to make full use of eID and trust services and outlines the options available to reach the objectives set by the political mandate from the President of the Commission and the European Council.

1.2 KEY CONCLUSIONS OF THE EIDAS EVALUATION

An evaluation on the functioning of eIDAS[33] was conducted as part of the review process required by Article 49 of eIDAS. The conclusions of the evaluation are summarised in the table below. These findings are further elaborated in the problem definition and linked to the problem drivers (see section 2)

Figure 1 - Key conclusions of the eIDAS evaluation

Electronic identification	
Effectiveness	1. Only a limited number of eIDs have been notified, limiting the **coverage** of notified eID scheme to about 59% of EU population 2. The **acceptance** of notified eIDs both at the level of Member States and service providers is limited - not all eIDAS nodes are up and running and a limited number of public services offer eIDAS authentication 3. The **interoperability** of a number of eID schemes has been achieved at EU level 4. Limited incentives for Member States and service providers to connect to the eIDAS infrastructure 5. Lack of **monitoring and reporting obligations** limiting the access to reliable data on active connections and usage of notified eIDs 6. The **actual cross border use** of eIDs is very limited but the evolution of the number of transactions in certain Member States confirms increasing trend in the usage of notified eID schemes since September 2018 7. Lack of **awareness** of eIDAS among citizens and the use of notified eIDs by private service providers 8. eIDAS based eIDs has not been able to expand sufficiently into the **private sector** 9. The **governance** model of eIDs is complex – lacks harmonisation of certification, review of the notification and peer review procedures, clarification on the security requirements, the tools and procedure to manage eID related incidents

[27] COMMUNICATION FROM THE COMMISSION on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, C(2020) 2800 final, 7.5.2020

[28] https://www.ecb.europa.eu/euro/html/digitaleuro.en.html

[29] Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU

[30] Regulation (EU) 2020/1056 of the European Parliament and of the Council of 15 July 2020 on electronic freight transport information

[31] https://ec.europa.eu/taxation_customs/general-information-customs/electronic-customs/eu-single-window-environment-for-customs_en

[32] Europe's moment: Repair and Prepare for the Next Generation, {SWD(2020) 98 final}

[33] [Reference]

Efficiency	10. The key stakeholder groups for which the eIDAS generated costs and benefits are national authorities, eIDAS node operators, eID providers and service providers. In charge of managing the system, national authorities and eIDAS node operators and eID providers bear significantly higher costs than service providers 11. The baseline assessment indicates that the quantifiable costs are higher than benefits due to a low uptake where benefits did not materialise. 12. For individual stakeholders, a considerable part are 'expected' benefits (discounted as future benefits) and therefore hardly quantifiable 13. Reducing uncertainty for the private sector, the centralization of the updates to eIDAS nodes and outreach activity for final users would lead to possible net cost reductions
Relevance	14. The current scope and focus on notified eID schemes Member States to enable access to online public services is **too limited and inadequate** 15. The vast majority of the needs of eID and remote authentication remain with the private sector 16. eIDAS does not address the needs of specific sectors (e.g. education, banking, travel, aviation) - one of the limitation factor is the lack of **specific attributes** by domains
Coherence	17. Lack of common understanding of the requirements in the level of assurance framework 18. The limitations of the eIDAS **minimum dataset** are an important shortcoming for the implementation of eIDAS solutions in a number of EU sectoral legislations 19. Lack of provisions for the mutual recognition of non EU-based eIDs
EU added value	20. The eIDAS Regulation has created incentives for Member States to deploy an eID solution but the added value with regard to eID is limited due to its low coverage, uptake and usage 21. The needs originally identified for the adoption of the eIDAS Regulation still **remain relevant**; repealing the Regulation would lead to fragmentation and negative consequences to other legislative areas that rely on eIDAS
Trust services	
Effectiveness	22. The eIDAS successfully established legal certainty on liability, burden of proof, legal effect and international aspects of trust services, but some issues remain 23. **Availability and take-up** of trust services in the EU have increased since the introduction of the eIDAS Regulation, there are differences among Member States and among different trust services 24. There is a **diversity of interpretation of the** requirements between Member States, which could be addressed by adopting non-mandatory implementing acts foreseen by eIDAS 25. eIDAS 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 26. Formalisation of the **cooperation between supervisory bodies** to improve implementation of the eIDAS
Efficiency	27. The key stakeholder groups in the area of trust services for which the eIDAS has generated costs and benefits are accreditation, conformity assessment, and supervisory bodies and qualified and non-qualified trust service providers 28. Recurring costs for governance are limited and mainly linked to ensuring compliance; QTSPs spent an average of EUR 800.000 to obtain and maintain the qualified status 29. 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) - TSPs register benefits in an extension of market base, reputational increase and better access to finance due to compliance with the high eIDAS standards
Relevance	30. The **objectives** of the eIDAS framework remain **adequate** to address the identified issues - 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 31. Need to define **new trust services** for eArchiving, requirements for the digitisation of paper documents and supporting portable identity credentials
Coherence	32. The provisions on the role of conformity assessment bodies lack sufficient details on their obligations, liability or level of competence 33. The quality of conformity assessment reports varies across the national supervisory regimes - more reliance on standards could deliver more harmonisation and prevent a regulatory race to the bottom 34. In some areas **divergent approaches at national level** have impacts on trust and a level playing field, e.g. Article 24(1)(d) which allows Member States to recognise certain identification methods (such as biometric verification)
EU added value	35. The 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.

1.3 THE DIGITAL IDENTITY MARKET CONTEXT[34]

A ***digital identity*** is a digital representation of a natural or legal person. It lets you prove who you are during interactions and transactions. ***Attributes*** contain information about a subject. This can include details such as your legal name or date of birth, as well as details from other organisations, such as your professional qualifications, bank balance or medical history. Today, it is considered that digital identities are also comprised of such characteristics or ***attributes*** related to an individual, an organisation or an electronic device. The information contained in a digital identity allows for the authentication of a user or the presentation of his/her digital attributes, giving him/her access to public or private services online or offline. The overall objective is to enable citizens and businesses to prove who they are or to prove their attributes/characteristics, without needing physical documents.

What is emerging in the market today is a new environment where the focus has shifted from the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities. For example, access to services may rely on the verification of qualifications or age (for example to buy alcohol online or enter a nightclub), or whether a person has been vetted. While the issuance and acceptance of such attributes require that the person has been identified, it is the attribute and the fulfilment of its requirements that provides access to specific services and therefore takes centre stage over the provision of digital identity. A digital identity system that does not allow a seamless link with attributes and credentials is therefore no longer addressing current societal demands due to digitisation.

Example 1 – authenticating to an online service proving who you are: Kurt has moved to a country where a large number of public services can be accessed online. To access the online service required for the submission of the annual tax return, Kurt needs to identify and prove that he is who he claims to be using a digital identity solution. Using the eID issued by his home country, he is able to access the service thanks to eIDAS. Due to the Single Digital Gateway Regulation, from December 2023 on, Kurt will also able to request from his home country the tax returns required to prove his income status from previous years, using the same eID.

Example 2-use of an attribute offline: Sarah is in the queue for a nightclub and the door security guard asks for her ID. Instead of showing her physical ID card, which contains lots of personal information, she instead uses her digital identity. She signs in on her phone using secure biometric authentication and shows the QR code to the security guard. The security guard can then scan this code, see it is a valid identity, and receive confirmation that Sarah is over 18 years old, without seeing any more details such as her date of birth or address.

Example 3-use of an attribute online: Carmen needs to travel to another country for work. She must provide a medical certificate before taking the job. Carmen will get the medical certificate that confirms she complies with the rules set by the employer. Whoever gave Carmen the certificate can add the information from this certificate as attributes to Carmen's personal data store app (sometimes known as a 'digital wallet'). This attribute (the medical certificate in this case) can be shared online with the employer before Carmen arrives in the country[35].

THE DEMAND FOR DIGITAL IDENTITY SOLUTIONS

Digital identification solutions, including the provision of digital certificates for attributes, have seen an increasing demand by business and users. One of the main benefits of using digital identity solutions is the potential for ***efficiency gains*** as it allows service providers to communicate with their customers online and cut costs[36]. The difference in cost of the online and physical channels can be threefold.[37] Given the increase in the pace of digitalisation of the economy and society, as shown by the COVID pandemic, online identification and the sharing of attributes is becoming more important as the number of identity-sensitive and personalised services increase. The ability to identify digitally is also of increasing importance for social inclusion.

---

[34] For an overview of market structure, please see annex 5, Chapter 1.

[35] Examples adapted from the UK Digital Identity and Attributes Framework

[36] For example, banking sector's digital champions' cost/income rate is 4 percentage points better and return on equity 1,9 percentage points higher than their incumbent peers. https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/financial-services/ce-digital-banking-maturity-2020.pdf

[37] https://www.fintechfutures.com/files/2018/10/Backbase_The-ROI-of-Omni-channel_Whitepaper-2.pdf

Access to ***public services and to certain sectors*** (health, financial etc.) require identification or exchanging attributes with a high level of security and trustworthiness, including in terms of data protection. Secure identification systems are thus sometimes required by law in those sectors.

In this context, users also demand convenience and user-friendliness, including mobile-based solutions[38]. This has led to the emergence of new digital identity solutions that are self-managed or managed by a third party, external to the service provider[39]. However, these solutions provide convenient access to ***some private online services***, and often offer a lower level of security and data protection. Yet, users are increasingly concerned about their security, data protection and privacy beyond access to public services and regulated sectors. Consumers have thus a limited choice of solutions that both protect personal data and are easy to use, as using identification services provided by online platforms requires the user to consent to data disclosure. Choices for businesses are equally limited as identification solutions offered by platforms are not commercially impartial while there are often no better alternatives for online service providers given the large customer-base and market power of platforms. Secure identification means are offered by some private providers such as banks (mainly in the Nordic countries) but are limited to national use.

The rapid digitalisation of services has also increased the demand for the provision of credentials digitally proving attributes such as medical certificates or professional qualifications. This is particularly the case in the education, banking, health or travel sectors[40].

Recent technological solutions offering security and user-friendliness are digital wallets. Commercial versions are typically linked to payment solutions (ApplePay, GooglePay etc.) and allow to store and link different data sets or credentials (such as payment data, transport tickets, student IDs etc.) in a single seamless environment on the mobile phone. The first public sector wallets are now available and typically combine identification credentials with other public services and documents[41]. Given the versatility and user convenience of digital wallets, many developers and providers of wallets focusing on identification and authentication have emerged[42]. Many solutions focus on delivering very specific services and some solutions combine public and private sector attributes seamlessly[43].

Example 4 – Digital Identity Wallet[44]: Peter has installed a Digital Identity Wallet on his mobile phone. It has been provided by his home country, ensuring that the wallet has been issued to him and no one else pretending to be him. Based on the use of highly secure components for the storing of data, Peter fully trusts that the Digital Identity Wallet is safe and can be used trusted. Peter has a driving licence, a university diploma, a vaccination certificate and a residences card he used to carry around as physical cards in the more traditional wallet. Now available as digital attestations, he stores them in his digital identity wallet. Using the wallet, Peter no longer needs to rely on third parties to ensure the security of his identity data, reducing the risk of fraud from large scale cyber security attacks targeting big firms holding identity data about millions of users. Using the Digital Identity Wallet Peter also stores his boarding cards and the digital passport recently issued by his home country.

PROVIDERS OF DIGITAL IDENTITY SOLUTIONS

Organisations including Grand View Research, Fortune Business Insights and Global Market Insights predict that the identity and access management market will grow globally to at least €17 billion[45] by 2026. Meanwhile, Gartner predicts that by 2023, identity solutions will be a multi-billion-euro industry[46].

The market of digital identity solutions in the EU is large and diverse. It includes public sector providers providing national eIDs under national law and sometimes under the voluntary interoperability framework

[38] Since 2016, mobile has overtaken desktop as the main means of accessing websites, with a market share of 53% in 2018: StatsCounter. (2020). Desktop vs Mobile Market Share Worldwide

[39] Gartner: Innovation Insight for Bring Your Own Identity (2019)

[40] See evaluation report, Q11.

[41] See for example the Polish CitizenWallet: https://www.gov.pl/web/mobywatel

[42] Examples of recent wallet developments include Thales (https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/digital-id-wallet), Idemia (https://www.idemia.com/mobile-id), Esatus (https://esatus.com/esatus-ssi-wallet-app-ab-sofort-fuer-ios-und-android-verfuegbar/?lang=en) and nettoken (https://nettoken.io/).

[43] See e.g. the Belgian private/public wallet 'ItsMe' https://www.itsme.be/fr/partners

[44] This example is hypothetical to demonstrate the potential of a Digital Identity Wallet.

[45] https://www.fortunebusinessinsights.com/industry-reports/identity-and-access-management-market-100373

[46] Gartner: Innovation Insight for Bring Your Own Identity (2019)

provided by eIDAS. Identity providers in the private sector include in the first place social media, which occupy the largest market share for digital identification and provide third-party identification services for a large part of service providers on the internet. Other private providers include banks and other financial service providers, telecom companies and mobile operators and dedicated networks and providers of digital identification[47]. While public providers largely focus on highly secure identity solutions for online access to public services, these solutions are not always mobile and user-friendly. Private providers typically focus on less secure solutions, except in areas where regulatory requirements apply (e.g. in the financial sector) but focus on convenience and a seamless user-journey.

Government eIDs (eIDs) are backed up by identity proofing according to strict rules and processes defined by governments, and therefore provide a high level of assurance on the link with the real identity of a person, making them currently more relevant for use cases that require a high level of trust. As these identities require a longer and more complex process to be issued, their usage tends to be more limited[48], including for cross-border use. Only those government eIDs that have been notified under eIDAS produce legal effects across borders. Despite increasing demand for secure and reliable digital identity means also to access private services, these types of identities are currently mostly offered for accessing public services.

A quick and easy way to create a digital identity is through a ***social media*** account, where identity is self-asserted and does not require further authentication processes. Many private online service providers rely on social media login to simplify authentication for the user, and to gain access to user data, if permission is given by the user. A recent Eurostat survey estimated that in 2020, 34% of EU citizens used social login to access online services[49]. The social login market features several market players such as Facebook (including Instagram), Google Sign-In, LinkedIn, Twitter and Amazon. These five have an aggregated market share of 87% of social logins in Europe[50]. The drawback is that being self-asserted, these identity solutions cannot be used to access services that require a higher level of assurance in the identity of the person, such as public services or banking, nor do they satisfy citizens' data protection expectations. Most recently, platforms and social media also seek to provide digital identity with higher levels of assurance, but mainly in connection with payment services, e.g. Apple Pay, Google-Pay or Libra / Facebook.

Banks are acting as service providers for digital identity proofing and are usually regarded as trustworthy organisations. Bank digital identity solutions have gained popularity especially in the Nordic countries, where they can be used not only for bank transactions but also for public digital services and for accessing private services in a wide range of sectors[51]. However, most bank digital identity services remain closed off to external service providers and digital services in the private sector[52]. ***Mobile network operators*** provide users with a SIM card that allows them to be identified within their specific mobile network. GSMA Mobile Connect offers a solution that enables people to identify and authenticate using their mobile phone[53] without a username and password, providing a globally interoperable solution made available by mobile network operators[54]. Finally, ***dedicated digital identity companies*** offer users the opportunity of creating a digital identity by following a registration process backed up by already existing ID documents (e.g. driving license, passport), social media identity, or other certificates, and at the same time increasing the security of these identities with biometric tools such as facial recognition. These solutions offer portability and employ advanced technologies such as biometrics to protect the identity. These service providers are sometimes recognised by Governments and their solutions notified under eIDAS.

A market for the ***provision of credentials and attributes*** has emerged in a number of sectors. Some Member States have developed proprietary systems or trust frameworks that allow e.g. for the expression of

---

[47] Gartner: Innovation Insight for Bring Your Own Identity (2019)

[48] Gartner (2019), Innovation insight for Bring Your Own Identity.

[49] https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisci_ip20&lang=en

[50] LoginRadius: Digital Identity Trends (2019)

[51] https://www.bankid.no/en/company/

[52] Gartner: Innovation Insight for Bring Your Own Identity (2019)

[53] https://www.gsma.com/identity/developer-portal

[54] As of August 2020, 23 mobile network operators have made the Mobile Connect authentication service available for their users, while a further 11 are piloting it. Major EU telecommunications providers already providing the Mobile Connect solution include Telefonica, Orange, Deutsche Telekom, Vodafone Germany, Telia, T-mobile, and KPN. See https://developer.mobileconnect.io/operators?title=&name_list=All&field_mobile_connect_status_value=2

ePrescriptions or digital driving licenses. Europass[55] develops a technical infrastructure to express credentials in the area of learning e.g. to create diplomas and certificates for students. The European Commission has proposed a Regulation for the provision of digital green certificates[56]. In the private sector, digital credentials have reached users in particular in the area of finance[57]. Private platforms offering personal credentials are only emerging but several wallet solutions linked to identification are in preparation[58].

See further details in Annex 5, chapter 1 on how eIDAS works, on the demand for digital identity solutions and on providers of digital identity solutions.

2 PROBLEM DEFINITION

2.1 WHAT ARE THE PROBLEMS?

State of play of implementation of eIDAS

As regards eID: Since the entering into force of the eID part of the Regulation in September 2018, only 14 Member States have notified at least one eID scheme[59]. As a result, 59 % of EU citizens have the possibility to use trusted and secure eID scheme across borders although only 7 schemes are entirely mobile responding to current user expectations. As not all technical nodes to ensure the connection through eIDAS are operational, cross-border access is limited[60]. In addition, on average only half of public services accessible online domestically can be reached cross-border via the eIDAS network. For example, using a notified eID to access an online public service of the tax authorities in another Member State may be denied because the back bone services of the tax authority have not been connected to the eIDAS Interoperability framework.

As regards trust services, there are currently 202 active qualified trust service providers[61] operating in 28 of the 31 EU and EEA/EFTA countries. Qualified eSignatures are the service provided most on the market (158), followed by qualified time stamps (114) and qualified eSeals (107). 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[62] at present.

Please refer to Annex 5, chapter 2 for more detailed information.

More than 5 years after the adoption of the eIDAS Regulation, mixed conclusions must be drawn on its success.

For ***trust services***, the eIDAS Regulation has created a European market with common rules for the supervision of Qualified Trust Service Providers and the creation of legal effect of e-signatures, e-seals, etc., across borders. Although there are some weaknesses in the harmonisation of supervisory procedures and in the implementation of Qualified Website Authentication certificates (QWACs), trust service providers confirmed to more than 70% that the Regulation had overall improved trust and confidence in the security, quality and availability of trust services[63].

For ***eID***, a more critical conclusion must be drawn based on a number of factors, partly related to the regulatory shortcomings of the Regulation and its implementation. More importantly, there have been

---

[55] https://ec.europa.eu/futurium/en/europass/europass-digital-credentials-infrastructure

[56] COM/2021/130 final

[57] ApplePay, GooglePay, LGPay, SamsungPay, FitBitPay, GarminPay .

[58] See e.g. Microsoft: https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/microsoft-decentralized-id-blockchain/amp

[59] BE, CZ, DE, DK, EE, ES, HR, IT, LV, LT, LU, NL, PT, SK, The United Kingdom notification of UK.GOV Verify (on 2 May 2019) is not included in this analysis. Four Member States have notified multiple schemes (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). By March 2021, 3 Member States (France, Malta and Sweden) had pre-notified additional eID schemes. Overview of pre-notified and notified eID schemes under eIDAS:https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[60] As identified by the eIDAS evaluation, in 2019 about 67% of nodes could receive identification requests from abroad although in principle full coverage should have been reached by September 2018 when mutual recognition applied for the first national eID scheme. In September 2020, only 22 out of 30 countries (27 EU Member States and Iceland, Norway, Liechtenstein) 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. In addition, although 19 eID schemes of 14 Member States had been successfully notified, not all of these 14 Member States had nodes with sending functions fully operational.

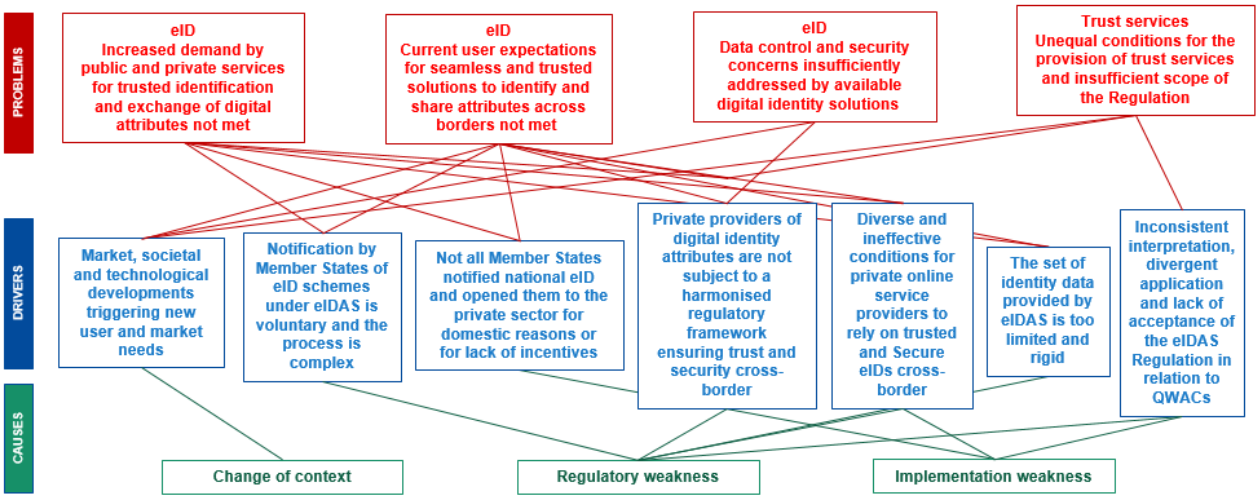
[61] State of play in April 2021: https://webgate.ec.europa.eu/tl-browser/#/dashboard

[62] BE, BG, DE, ES, FR, NL, SI,

[63] See eIDAS evaluation, chapter 5.

fundamental changes in what users come to expect, in technological developments, and in changes to the market given the sharp increase in number of services online and a shift away from the reliance on digital identify alone to the provision of digital attributes. Moreover, there is also a shift towards more user centric electronic identify solutions and solutions allowing users to control all aspects of their digital identity and protect personal data.

Figure 2 - Problems, drivers and causes



INCREASED DEMAND BY PUBLIC AND PRIVATE SERVICES FOR TRUSTED IDENTIFICATION AND EXCHANGE OF DIGITAL ATTRIBUTES NOT MET

The eIDAS Regulation focuses on access to cross-border public sector services, and has been able to offer this access only for a limited number of them (see below). However, since its adoption in 2014, the demand for secure and trusted identification and exchange of attributes has increased fundamentally both for access to public and private services.

As regards the ***private sector***, market demand for trusted and secure identification has substantially increased in sectors such as finance, transport or health. This is due to the general evolution of digital transformation and the fact that simplification of processes and considerable cost savings are possible thanks to a link of private sector use-cases with secure and trusted eID. This includes for instance facilitating a fully online customer on-boarding process in banking and insurance with a high level of security and data protection.

However, cross-border private sector use cases using government eIDs notified under eIDAS are currently very limited[64]. Even if the Regulation encourages Member States to allow private online service providers to offer the possibility to authenticate using a notified eID, not all notified eIDs are allowed to be used by the private sector even at national level. In 2018, eID schemes of 12 Member States could be used by the private sector at national level[65]. For example, in the Czech Republic[66], holders of the national eID can use it to access health insurance companies[67], online gaming and betting websites[68], and a law firm[69] on top of eGovernment services. The Danish NemID can be used to authenticate to online banking[70]. In Germany, the list of authorised relying parties is also published and includes banks, notaries, pension insurances and system providers for accountants and attorneys[71].

---

[64] The usage by the private sector is limited because there is no compulsory acceptance for the private relying parties, as it is the case for the public sector mutual recognition.

[65] In a consultation of EU-28 national experts in June 2018 conducted by the European Commission, at least 12 EU Member States declared that they allow the reuse of at least one eID scheme by domestic private relying parties for national transactions. Nine among them have declared that they will open this possibility to private relying parties established outside their national territory. At the same time, four Member States shared that they are currently not allowing the reuse of their national eID scheme authentication service by private relying parties at the national level and will unlikely allow this possibility to private relying parties established outside their territory.

[66] Identita.cz, Qualified online service providers, see : https://www.eidentita.cz/Home/Ovm

[67] https://www.ozp.cz/ and https://portal.cpzp.cz/

[68] https://www.sazka.cz/

[69] https://www.ak-vych.cz

[70] https://www.netbank.nordea.dk/netbank/index.jsp + https://danskebank.dk/privat/find-hjaelp/netbank-letbank-og-apps

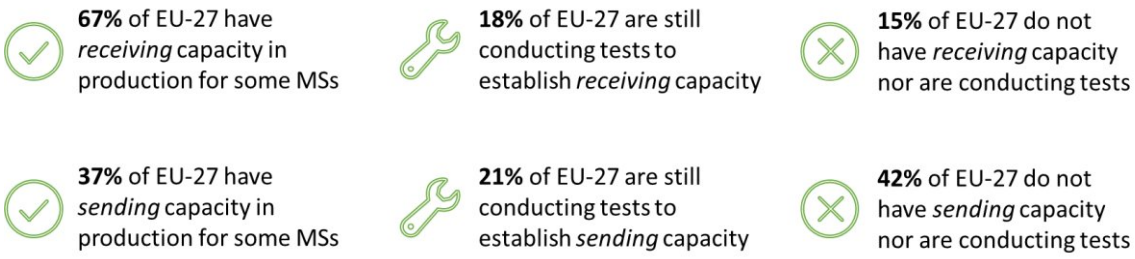
[71] Bundesministerium des Innern, für Bau und Heimat, Granted authorization certificates, see: https://www.personalausweisportal.de/DE/Service/Downloads/Erteilte_Berechtigungszertifikate/Erteilte_Berechtigungszertifikate_node.html

Overall, the eIDAS evaluation shows that cross-border use of notified eIDs by the private sector is practically inexistent due to questions of liability and the lack of viable commercial models, complexity of connecting to the nodes and limitations of the person dataset (See below in the drivers section).

eIDAS indeed cannot address these new market demands given its inherent limitation to the public sector, the complexity for online private providers to connect to the system, its insufficient availability in all Member States and its lack of flexibility to support a variety of use cases (see section on drivers). Furthermore, identity solutions provided outside eIDAS cannot seamlessly respond to the new market needs. As mentioned in section 1, social media providers cannot offer a direct link to trusted and secure eID today, which is essential for legal certainty and to address e.g. liability issues. Their offers are therefore limited to certain private sectors such as e-commerce. While certain private providers, such as Banks, are able to offer digital identification and authentication with higher levels of assurance, their services remain closed to their own customers or, in those cases where they are also offered to external users, such identification means do not benefit from cross-border legal recognition which limits use cases and prevents scaling-up[72]. In addition, the inability to offer secure and trusted eID for the private sector and to link them to attributes and credentials limits the competitiveness of EU digital industry developing independent e-commerce platforms and online services linked to trusted eID, such as in banking health or other areas where identification is sensitive. In the absence of a rules-based framework, online platforms equipped with large market power are likely to occupy this part of the market. As regards access to ***public services***, demand has also evolved due to digitisation. An increase in mobility (about 30% of EU population travel yearly to another Member State) and changes in user needs and preferences point to an increase in the demand to access public services online across borders. However, eIDAS focuses mainly in the needs of those EU citizens of working age residing in another EU Member State, which represents in number only around 3% of EU population[73].

Moreover, the core purpose of eIDAS, to enable the cross-border access to those public online services could also not be entirely fulfilled. Even in those Member States which notified a national eID under eIDAS, substantial barriers to access public online services persist. 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[74].

Figure 3 - eIDAS node sending and receiving capacity across EU



Only 14% of providers of seven key public services across all Member States allowed cross-border authentication with a notified eID. The overall number of services connected to the national nodes is considerably smaller than the number of services available for access via the domestic eID schemes. Data provided by Member States on the number of public service providers connected to eIDAS nodes is very different: While Belgium reports for 2018 over 1000 public service providers, Germany reports 95 service providers for 2020 (*additional data in Annex 5*).

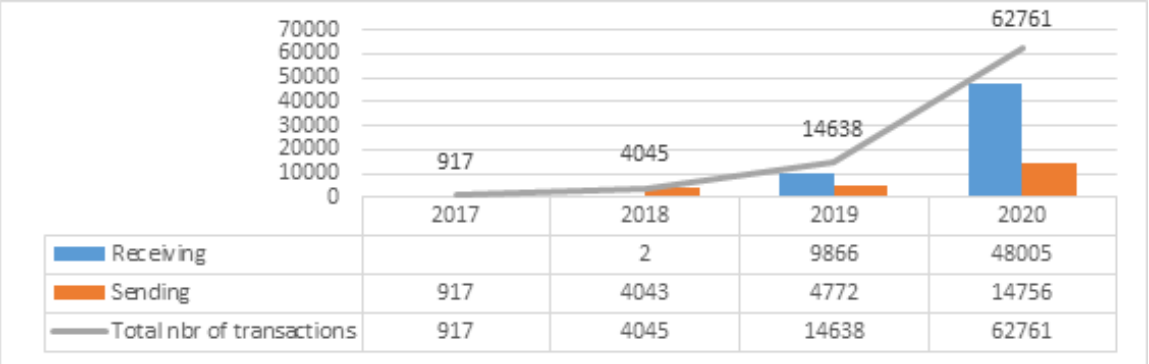
The number of cross-border authentications and especially the number of receiving transactions provides an estimate on the current usage of notified eID schemes, as it is related to the number of use cases where citizens request access to an online service across borders.

[72] Examples include dedicated digital identity companies, such as Onfido or WebID.

[73] https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

[74] Evaluation report, page 22

Figure 4 - Evolution of the number of yearly cross-border authentications in Austria, Czechia, Estonia, Netherlands, Luxembourg, and Sweden



	2017	2018	2019	2020
Receiving		2	9866	48005
Sending	917	4043	4772	14756
Total nbr of transactions	917	4045	14638	62761

eIDAS cannot fulfil the current demand due to implementation weaknesses in the deployment of the eIDAS interoperability framework, difficulties in identity matching[75], but also due to failure of granting access to a large number of public online services by Member States to users identifying from abroad with an eID notified under eIDAS.

As regards the ***market demand for credentials digitally proving attributes,*** such as medical certificates or professional qualifications, they are currently not covered by eIDAS. Member States and service providers have therefore been forced to develop proprietary trust and interoperability frameworks to ensure the security of these services and/or their recognition across borders. This includes health (ePrescriptions or medical certificates), travel (facilitating travel and border control through information in electronic machine readable documents) and education (Europass Digital Credentials)[76]. 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[77] and the Horizon 2020 project Future Trust has also piloted[78] the possibility to combine academic ID and national ID in order to issue trustworthy certificates for creating an EU Student eCard[79]. A recent example is the ***Digital Green Pass Regulation***[80], which foresees the development of an independent interoperability and trust framework for cross-border travel certificates by mid-2021.

Example 5 – Attributes / Credentials: Digital Identity can provide trust and security to attributes and credentials in various areas. An EU-wide trust framework for attributes and credentials linked to strong identity verification would for example be able to protect sensitive health data and facilitate its exchange across borders upon user consent. In the absence of an existing EU framework for the attestation of digital attributes and credentials linking them to trusted eID, a specific regulatory framework for the swift provision of certificates to prove medical test results ("Digital Green Certificate") has been necessary in March 2021.

CURRENT USER EXPECTATIONS FOR SEAMLESS AND TRUSTED SOLUTIONS TO IDENTIFY AND SHARE ATTRIBUTES ACROSS BORDERS NOT MET

Users today expect seamless online journeys, mobile applications and single-sign-on solutions that can be used for online services in the public and private sector, covering all use cases for identification ranging from pseudonymous log-on to an online platform to secure identification for e-health or e-banking. Secure online identification and the exchange of attribute credentials is becoming more important as the number of identity-sensitive and personalised services increases. The ability to identify digitally will become an important factor of social inclusion and the provision of digital identity a strategic asset.

---

[75] Problems related to identity matching can prevent citizens using a notified eID from accessing online public services in cases when the unique identity of the person cannot be established, or when a person cannot be uniquely linked to an existing record in another Member State (see below in the Section on Drivers).

[76] https://ec.europa.eu/futurium/en/europass/europass-digital-credentials-infrastructure

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

[78] 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/

[79] https://ec.europa.eu/digital-single-market/en/eu-student-ecard

[80] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate), COM/2021/130 final

New technological solutions are adopted by the public and private sectors that aim to address the evolving needs of citizens and businesses. ***Self-sovereign identity (SSI) solutions*** offer a user-determined environment that facilitates data protection and control. Digital wallets are a practical way of implementing SSI as they offer convenient possibilities for the user to manage and exchange their own identity-related information, attributes and credentials. Some Member States are moving into this direction, which, unless regulated at EU level, will further increase the disparity between national systems.

However, today many citizens do not even have access to trusted and secure ***government eID means*** allowing them to access services across border. Six years after the adoption of eIDAS, the eIDAS framework covers only about half of the EU population[81], leaving 41% of EU citizens without the possibility to use any trusted and secure eID scheme across borders.

Some Member States have involved the ***private sector in the provision of eID means*** and their services are recognised and used for access to online public and private services. However, their cross-border recognition relies on a decision by Member States to notify them under eIDAS. So far, only few have recognised private schemes, notably Belgium (ItsMe), Italy (SPID) or Sweden (BankID).

Alternative ***digital identification solutions by private providers***, not recognised by governments, do exist (see section 1.3). However, as mentioned above they only address some private use cases not requiring high level of security. Other more secure solutions offered by private providers lack common frameworks or standards as regards for example, the levels of assurance that they provide. They can therefore not scale up and be recognised across borders for access to public or private services which require a certain level of trust.

Without access to seamless and trusted identity solutions recognised cross border, citizens and businesses will have to rely on solutions that are not linked to their legal identities issued by Member States and are therefore less secure. This contradicts the increasing user demand for a secure digital identity to access all online services in the EU that gives users control over the use of their personal data and allows for the exchange of personal data attributes and credentials.

DATA CONTROL AND SECURITY CONCERNS INSUFFICIENTLY ADDRESSED BY AVAILABLE DIGITAL IDENTITY SOLUTIONS

There are security risks involved in providing personal data online or in information systems for authentication purposes. A data breach occurs when a cybercriminal infiltrates a data source and extracts confidential/private information, and many security incidents mainly affect personal data. For example, in April 2021 it was reported that data including phone numbers, Facebook IDs, names, birthdates and in some cases, e-mail addresses from 500 million Facebook users had been leaked online[82].

An average person has more than 90 user accounts (digital identities) online. Having many accounts leads to reusing passwords, which increases the risk of identity theft and the leaking of personal data. In 2019, over 4.1 billion personal data records were exposed due to data breaches. Email addresses were exposed in 70% of reported data breaches and passwords were exposed in 65% of reported data breaches. A recent Eurostat survey showed that 75% of EU citizens use low-level security identity tools provided by the private sector (e.g. password and username or email address) with potential risks to the integrity of personal data or even identity theft. According to a Gigya survey, more than 80% of consumers admit to having quit an online registration form because they were uncomfortable with the amount or type of information requested. A recent Eurobarometer survey shows that 88% of consumers wish for more control over their data[83].

However, neither public nor private offers fully respond to this demand. Existing eID under eIDAS is not sufficiently widely usable for identification in the private sector to represent a viable alternative and has inherent limitations to discretional data disclosure for the user. In addition, identification provided by large online platforms often does not allow for the effective protection of personal data, as evidenced by major data breaches and enforcement actions over the last decade, but is used by service providers given the large market power and customer base of platforms:

Platforms and social media allow users to authenticate to third-party applications using their social network profile. They frequently require that users sign up to/register with the platform's own service in order to use

[81] In theory, 59% of the EU population currently has access to a notified eID scheme, see evaluation SWD, p. 25

[82] https://www.businessinsider.fr/us/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

[83] Eurobarometer 503, Attitudes towards the impact of digitalisation on daily lives, December 2019

another of its products (e.g. an operating system, social network, etc.)[84]. Although the GDPR applies, data management, including activity data management, is not transparent in these situations and often the user has no other option than to consent to the disclosure of data in return for using the platform's identification service. As mentioned by the European Data Protection Supervisor:

> *"[t]he concern of using data from profiles for different purposes through algorithms is that the data loses its original context. Repurposing of data is likely to affect a person's informational self-determination, further reduce the control of data subjects' over their data, thus affecting the trust in digital environments and services"*[85].

While ***eIDAS notified eIDs*** offer a high level of security, it has limitations as regards the principle of data minimisation. For authentication to online public services cross-border, it is compulsory to exchange the full minimum eIDAS data set and there is no possibility for the user to limit the transmitted personal data to the minimum required for a specific transaction. For example, eIDAS does not support so called ***"zero-knowledge claims"***, which allow a user to certify that he or she is above 18 years of age, without having to disclose her/his date of birth. Currently, even national eIDs offering a high level of security do not allow users to store data securely in the same place and apply full control on data release. Overall, eIDAS today cannot respond to user expectations for full control of personal data, and also private alternatives do not offer this possibility. The general shift towards a more comprehensive identity ecosystem that integrates attributes and credentials, some of them carrying sensitive data such as in the health sector, makes it necessary to develop eID ecosystems that are able to effectively protect personal data and offer full user control.

UNEQUAL CONDITIONS FOR THE PROVISION OF TRUST SERVICES AND INSUFFICIENT SCOPE OF THE REGULATION

Although the evaluation of the eIDAS Regulation concludes that the regulatory framework has successfully established legal certainty on liability, burden of proof, legal effect and international aspects of trust services, it also shows that there is room for improvement regarding a harmonised application of ***supervisory procedures*** and ***processes for identity proofing***, in particular when these processes are carried out remotely. Trust service providers (TSPs) must verify, in accordance with national law, the identity of the natural or legal person to whom a qualified certificate is issued. Since 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.

In addition, there are national differences in the way the conformity assessment of qualified trust services providers is carried out, which requirements apply and which standards are used. As the eIDAS Regulation does not regulate these aspects, differences in the application of the rules for national supervision between Member States raise challenges regarding a comparable level of trust and security of the services provided and of a common level playing field. For example, the evaluation shows that less than 50% of the Qualified Trust Service Providers reference specific standards (such as ETSI EN 319401) to prove compliance with the Regulation. Furthermore, only 15 Member States have introduced specific national procedures for the qualification of trust service providers. In other Member States, the lack of procedures creates uncertainty as to the criteria against which the trust service provider has been evaluated to ensure conformity with the Regulation. As regards the different practices in conformity assessment, the lack of a more harmonised approach to auditing with regards to the form and content of the conformity assessment reports has caused, according to ENISA[86], some "incongruences in the qualifications of TSPs in different countries as well as their qualified trust services, undermining trust and confidence".

The problems described for the provision of trust services are also linked to the absence of a common governance structure at EU level similar to that of the Cooperation Network for eIDs allowing Member

[84] DMA Impact assessment - SWD(2020)363 final

[85] EDPS Opinion on online manipulation, Opinion 3/2018, 19 March 2018, p. 15 and EDPB report on social media and impact of profiling on competition, page 7

[86] ENISA study of January 15, 2019: Towards global acceptance of eIDAS audits; https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits

States to jointly address them. In the evaluation, some supervisory authorities noted that the role of FESA[87] should be formalised to address the need of consistent application of eIDAS chapter on trust services in all Member States. Currently, FESA is an unofficial body and its activities depend on the initiatives of the representatives of the national bodies.

Risks of market barriers have also been identified for ***eArchiving services***. The eIDAS Regulation requires archiving the signatures of electronic documents but does not specify requirements and which standards to use. This has led several Member States to develop competing national rules. As part of the consultation process, a number of Member States and the majority of trust service providers consulted suggested expanding the eIDAS Regulation to a new trust service for eArchiving.

There is also need for improvement concerning the efficiency of a particular trust service, the provision of ***Qualified Website Authentication Certificates (QWACs)***. QWACS have been created by the eIDAS Regulation to enforce EU rules on a 'right to know' regarding the identity of websites[88]. 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 entity behind a website is required by law.

Despite the introduction of these certificates by the eIDAS Regulation, web browsers refuse to include them 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.

Alternative solutions to QWACs, such as TLS certificates applied by web browsers, 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.

In particular for websites run by intermediaries or trading companies[89] only QWACs can guarantee identity of the entity behind a website with a high level of assurance. The lack of recognition of QWACs by web-browsers may also conflict with the protection of fundamental rights of consumers as enshrined in articles 12, 101, 102, 114 and 169 of the Treaty on the Functioning of the European Union and with EU Consumer protection legislation, in particular Directive 2005/29/EC[90].

2.2 WHAT ARE THE PROBLEM DRIVERS?

The following problem drivers are linked to three dimensions, which intersect and reinforce each-other: regulatory shortcomings, implementation weaknesses and changes in context. These links are indicated as appropriate below.

MARKET, SOCIETAL AND TECHNOLOGICAL DEVELOPMENTS TRIGGERING NEW USER AND MARKET NEEDS (CHANGE OF CONTEXT)

[87] The Forum of European Supervisory Authorities (FESA) for trust service providers, is a forum open to national bodies responsible for supervision and/or trusted lists in accordance with the eIDAS Regulation. The scope of FESA is to support the cooperation, information and assistance among the members and to facilitate the exchange of views and agreement on good practices: http://www.fesa.eu/

[88] This 'right to know' is established in articles 2 and 3, 12, 101, 102, 114 and 169 of the Treaty on the Functioning of the European Union and article 5 section 1 letter (b), article 6 section 1 letters (b) and (c) and article 8 section 4 of the 2011/83/EU Directive on consumers rights. In order to allow consumers and all other interested parties to know the identity and reliability of a company and have full access to the most relevant information concerning a company, Member States are bound by article 14 of the Directive 2017/1132/EU that codifies certain aspects of company law.

[89] Following the definition of article 1 of the 2011/83/EU Directive on consumers rights.

[90] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices, protecting the right of consumers to know the legal entities they are interacting with, their geographical location to the point that providing misleading/inaccurate information or no information at all on the true identity of the business/trader, amounts to misleading or aggressive commercial practice (and fall just short of consumer fraud).

The context for the eIDAS Regulation in 2021 is fundamentally different to 2014, the year of its adoption. Various developments have created new demands that cannot be answered effectively by the eIDAS Regulation in its current form. The following elements summarise these developments, which are also referenced in other parts of the impact assessment as strong and overarching factors of change:

- With the ubiquity of smartphones, the overall progress in digital transformation and the emergence of new user determined technologies such as self-sovereign identity, users expect to identify online and mobile with a single log-in solution using the same eID for public and private use-cases as confirmed by Eurobarometer data (see above).
- The push for further digitalisation in public administration and the economy accelerated by the ongoing pandemic[91] has created emerging offers for a variety of digital credentials and attributes to affirm personal and professional situations, claims and entitlements in a digital form. Today, these offers cannot relate to an overall technical and legal interoperability framework that inspires trust and security through the link to public eID and a focus on the protection of personal data. For this reason, the public sector pursues the development of various proprietary and insular solutions, for example in eHealth.
- In the private sector, large online platforms are preparing to offer digital identities at higher levels of trust and assurance, such as personal digital wallets, typically connecting identity attributes with payment credentials.

These developments of the market, technological and societal change and a shift in user behaviour and expectation described in the second problem (Current user expectations for seamless and trusted solutions to identify and share attributes across borders not met) are factors that reinforce each other and create a strong pull-effect for a personal, seamless, user-determined digital identity platform that allows to share different forms of identity data under full user-control.

Built on trusted and secure national eID, the eIDAS Regulation is in a privileged place to respond to these developments with a user-controlled personal digital tool that allows for the linkage of national eID and private and public credentials in a seamless way.

NOTIFICATION BY MEMBER STATES OF EID SCHEMES UNDER EIDAS IS VOLUNTARY AND THE PROCESS IS COMPLEX (REGULATORY WEAKNESS)

The ***absence of a regulatory obligation*** for Member States to notify a national eID scheme and submit it to the mutual recognition process is identified in the evaluation as a decisive factor for the problem that not all EU citizens and businesses can have secure identity means to access online services securely in a cross-border context. The introduction of a mandatory requirement, in the Single Digital Gateway Regulation, to use notified eIDs from December 2023[92], seems to have triggered the recent increase in the number of notifications[93].

Member States mostly agree on the outcome of the evaluation of the eIDAS Regulation showing that a strong push is needed to accelerate the pace of notifications.

Moreover, ***the notification process is long, complex*** and suffers from inconsistent interpretation and application of the mutual recognition requirements. Multiple stakeholders consider the peer review processes as cumbersome and inefficient[94]. A key aspect of inconsistent interpretation among Member States concerns the requirements for levels of assurance. To support mutual recognition of national eID schemes under eIDAS, Implementing Regulation 2015/1502 defines three levels of assurance - low, substantial and high – and establishes minimum technology-neutral requirements and procedures to achieve compliance. However, there has been disagreement among Member States how these requirements should be interpreted in practice,

---

[91] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#

[92] Articles 13 and 14 of Regulation (EU)2018/1724 requires Member States to ensure cross-border access to a number of online procedures by means of eID, eSignatures and eSeals from 12 December 2023 on.

[93] Sweden, France and Malta pre-notified in late 2020/early 2021.

[94] For instance, more than 1 in 4 respondents to a survey of Member States developed for the evaluation of eIDAS disagree with the statements "The mandate, working methods and operation of the Cooperation Network are adequate" and "The Cooperation Network has been effective in completing its mandated tasks". Position papers review and other survey and interview data collected suggest this is a widely shared view among stakeholders.

and there is no commonly agreed methodology for demonstrating compliance[95]. The lack of references to relevant standards in the implementing act negatively affects the effectiveness and efficiency of the process to achieve mutual recognition and therefore the availability of trusted and secure eID solutions. These weaknesses particularly affect mobile schemes, which benefit from high convenience and user uptake.

Currently it takes on average 9 months from the pre-notification[96] of an eID scheme until its publication in the Official Journal of the EU. In addition, there is a 12-month delay for the application of mutual recognition following such publication. Hence, it takes almost 2 years for citizens and businesses to take advantage of cross-border authentication.

NOT ALL MEMBER STATES NOTIFIED NATIONAL EID AND OPENED THEM TO THE PRIVATE SECTOR FOR DOMESTIC REASONS OR FOR LACK OF INCENTIVES (IMPLEMENTATION WEAKNESS)

In March 2021, the intention to notify national eID under eIDAS remained unclear for ten Member States[97]. This diverse group includes countries with eIDs at different stages of development at national level.

The reasons for not notifying existing schemes are diverse and cannot be determined clearly in all cases given the lack of structured information[98] and the fact that notification is voluntary and a political decision by each Member State. It is likely that for some Member States, existing eID schemes are not considered sufficiently technically mature to ensure interoperability with other national schemes within eIDAS[99]. For some other Member States, the system of mutual recognition, which is technologically neutral and based on functional security requirements, leaves a relatively wide margin of interpretation in relation to security levels that can be reached by certain technologies (e.g. mobile eID schemes). In addition to the absence of strict rules and requirements for the peer review process, outcomes are to a certain degree unpredictable which may act as a disincentive for notification. For other Member States, the necessary national regulatory frameworks may be absent or under review[100]. In addition, the low overall number of accessible public online services abroad act as addition disincentive. Ultimately, investments into infrastructure are required to upgrade existing eID, which also raises questions of technological choice considering existing legacy systems and given the absence of accepted standards at European level. As a result, the current system of eIDAS, based on ensuring interoperability through nodes is still not entirely operational, although all Member States are required to accept incoming identification requests from eIDAS (see summary above).

Even if all Member States would notify swiftly, the existing framework based on mutual recognition of eIDs is not fit for purpose considering the current shift towards the reliance on verified digital attributes and credentials. For the provision of attributes and credentials, a federated system of IT nodes based on technological neutrality and mutual recognition is not practical. It is unlikely that the diversity of use cases and high number of attributes and credentials in different areas can be bound efficiently into the exiting interoperability system, even if this is upgraded. Technical shortcomings associated with such a solution, like response delays or denials of service would act as a strong disincentive to private providers using the system and could not offer the same seamless user-journeys than the standards-based systems the private sector is developing.

One of the limiting factors affecting Member States incentives to notify eID schemes stems from the limited scope of the eID framework, which focused on very limited public sector use cases, mainly those to address the needs of EU citizens residing in another Member States than their country of origin. Although a rapid increase of digitalisation has triggered an increase of demand to access cross border online public and private services where user authentication is needed, the current shift to attributes and credentials which cannot be expressed by the existing eIDAS system may act as a disincentive for notification.

Although Member States can also notify or recognise private identity solutions only few have done so. Entrusting a private provider with operating a national eID is a sensitive political choice and issues of costs and liabilities, competition, interoperability with eGovernment services, trust and reasons of national sovereignty may be engaged. When Member States have functioning eID schemes provided by the private sector (e.g. banks or telecom companies), they might hesitate to notify those schemes since it would imply

[95] eIDAS evaluation study, p. 52

[96] Prenotification is a step preceding the notification where MS submit the draft notification documents to be assessed in the peer-review

[97] These Member States included: AT, BG, CY, GR, HR, HU, IR, PL, RO, SI.

[98] One of the identified shortcomings of the regulatory framework, in particular for eID part, is the lack of monitoring and reporting obligations.

[99] This may apply e.g. to e.g. CY, EL, IE.

[100] This may i.e. include AT.

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.

In addition, eID schemes notified by some Member States do not always cover all levels of assurance with the result that not all online public services abroad will be accessible for users of this Member State[101]. Several Member States have notified only smart-card based eID schemes. These systems are not fully mobile and their take-up at national level is limited.

Notified national eID schemes are not by default open to the private sector and the eIDAS Regulation does not include a requirement for this purpose. Even if the Regulation encourages Member States to allow private online service providers to offer the possibility to authenticate using a notified eID, few notified eIDs are allowed to be used by the private sector on national level and none on cross-border level for questions of costs and liabilities and technical issues of connecting private service providers to eIDAS nodes.

PRIVATE PROVIDERS OF DIGITAL IDENTITY ATTRIBUTES ARE NOT SUBJECT TO A HARMONISED REGULATORY FRAMEWORK ENSURING TRUST AND SECURITY CROSS-BORDER (REGULATORY WEAKNESS)

Currently, eIDAS exclusively regulates government eID solutions or solutions by private eID providers that are notified and guaranteed by a Member State[102]. Other digital identity solutions do not provide official identities of a person and in most cases are not recognised by governments, banks or telcos[103].

Identification attributes issued by the private sector (e.g. banks) are not covered by the eIDAS regulation and operate without legal effects across borders and without legal certainty about liability or transparency over security levels. Services have arisen both in the public and private sector to enable citizens to prove who they are or to prove their attributes/characteristics, without the need to provide physical documents. However, their cross border legal effect and the level of security is not ensured as a legal framework for this purpose is missing.

The identification of objects and devices follows international standards, which are out of scope of eIDAS. However, scenarios where things and IoT devices need to be linked in a trusted way to owners are increasingly frequent and can be achieved by linking attributes and credentials to secure and trusted eID. The absence of a regulatory framework at EU level for the provision of trusted and secure attributes and credentials also affects the possibilities to link IoT devices to trusted and secure eID of physical or legal persons. The number of connected devices installed globally could more than triple from 23 billion in 2018 to over 75 billion in 2025[104]. Traditional identity solutions focus exclusively on people and are not built for linking people and devices. Consultations with Member States and industry representatives stressed the need for a trusted and secure link between the identification of devices and the identities of physical and legal persons in order to protect against cybersecurity attacks of novel technologies, such as IoT, autonomous driving, 5G or smart devices[105]. For example, there are emerging use cases linking devices to their owners. Electronic certificates linked to a car can be stored on a mobile device and by means of encryption allow the user to open it and drive. The portability of such certificates would also allow him to pass it on for use by others. Relying on international standards establishing the identity of things, once linked to a person using attribute certificates, the digital identify wallet environment will allow the user to securely store multiple keys from numerous providers.

Example 6 - IoT: Marta just purchased a new car allowing her to open and start it using an App provided by the car manufacturer. She has also a boat, a scooter and a mobile home, the producers of which have issued Apps allowing her to operate them. However, the various producers use different procedures to link the

[101] The minimum level of assurance for incoming identification requests is determined at national level. For instance, if the required level of assurance is 'high' an eID notified at level 'substantial' will not be able to access the service.

[102] Article 7(a) of the eIDAS regulation

[103] There are examples where social logins are implemented by governments for certain non-sensitive public services that do not require a legal identification of the user – see: https://toolbox.estonia.ee/

[104] 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

[105] 33% of all respondents to the OPC on eIDAS considers that the revision of eIDAS must include provisions of identification of non-human entities (e.g. AI agents, IoT devices)

devices to Marta and to the device she controls, some of which are not entirely trustworthy risking theft. Moreover, the many proprietary solutions prevent her from keeping the device identity attribute certificates in the same wallet, ensuring the same level of trust and security provided to other type of digital identity attributes (diplomas, driving licences etc.).

DIVERSE AND INEFFECTIVE CONDITIONS FOR PRIVATE ONLINE SERVICE PROVIDERS CANNOT RELY ON TRUSTED AND SECURE EIDS CROSS-BORDER (REGULATORY AND IMPLEMENTATION WEAKNESS)

The limited reliance on notified eIDs by private online service providers is mainly due to two reasons[106]. First, each Member State remains free to set the conditions for the use of its national eIDAS infrastructure by private online service providers, leading to diverging national approaches. In addition, there is no guidance at national or EU level on pricing[107] (including revenue-sharing mechanisms), liability and support structure, responsibility for billing and payments and dispute resolution mechanisms[108] related to private sector use of notified eIDs. The impact assessment supporting the original proposal for the eIDAS Regulation already noted that, for example, pricing and liability rules for use by private services are set by the notifying Member State and differ considerably, with the result that only very few private services are connected to the eIDAS network[109].

Second, limited use by the private sector is due to lack of common standards of notified eID means which requires a connection via nodes and cannot offer a swift and seamless user-journey. Even if all notifying Member States potentially opened their eIDAS nodes to the private sector services providers across the Union, the diversity of national conditions for the use of the national eID infrastructures will still make it very difficult for the service providers to build a sustainable business plan or to accurately estimate the potential of this openness to expand their business cross-border. Overall, the lack of harmonised rules prevents the cross-border and cross-sector use of eIDs by the private sector, limiting the usability of notified eIDs.

"...key factors for the private-sector take up of formal eIDs therefore depend on: a) the availability of open technical systems b) the establishment of clear rules for use of eIDs and for eAuthentication processes c) the establishment of clear liability rules." [110]

THE SET OF IDENTITY DATA PROVIDED BY EIDAS IS TOO LIMITED AND RIGID (REGULATORY WEAKNESS)

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. Given the focus of eIDAS for public service identification, there is no possibility for the user to add additional data that is necessary in order to access certain private sector services[111] or to facilitate compliance with specific sectorial regulatory requirements[112]. The number of cases for which notified eIDs can be used are therefore in practice limited.

In contrast, 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 GDPR introduced the concept of 'privacy by design'[113], making explicit reference to data minimization. On top of this, it introduces the obligation of privacy by default, going a step further into stipulating the protection of personal data as a default property of systems and

---

[106] eIDAS evaluation report page 23

[107] Currently, relying on a notified eID scheme to access public services is free of charge

[108] GSMA. (2018). Mobile Connect for Cross-Border Digital Services Lessons Learned from the eIDAS Pilot. https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-Final.pdf

[109] Evaluation Study, p. 82

[110] Ducastel, N. et al. (2012). Study on Impact assessment for legislation on mutual recognition and acceptance of e-Identification and eAuthentication across borders. European Commission. https://ec.europa.eu/digital-single-market/en/news/study-impact-assessment-legislation-mutual-recognition-and-acceptance-e-identification-and-e

[111] For example, the financial sector may need proof of nationality, address or occupation, not currently under the minimum data set provided by notified eIDs

[112] E.g. the Payment Services Directive requires additional attributes such as 'country of tax residency' as part of the Customer Due Diligence processes.

[113] As per Article 25(1) of GDPR

services. The current eIDAS system does not allow the user to actively enforce these provisions in the GDPR and to control which data to share and with whom.

In addition, the rigid data set for notified eIDs makes it also difficult to ***match identity*** records as the current minimum dataset is often not sufficient to uniquely identify a person[114]. Such difficulties typically occur when a person owns different notified eIDs which makes matching the identity to a record difficult using automated means. Problems of identity matching limit the usability of notified eID and is predominantly linked to the cross border use of eIDs since at national level citizens can more easily be identified relying on national identifiers and unique national data sets[115].

Some service providers require a national registry number to grant access to online public services in order to avoid identity matching problems. However, not all Member states issue such a number and include it in the data set. Obtaining it may require physical presence which is an obstacle for users from abroad even in case they are eligible to obtain a national registry number and to access a service.

Several Member States have identified identity matching as a key challenge for the revision of the eIDAS Regulation. Full assurance on record matching / identity matching is a precondition for a seamless cross-border functioning of a European Digital Identity for persons, companies and devices[116]. Without full assurance on identity matching, Member States will be reluctant to open services and agree to an extension of eID / eIDAS to the private sector.

INCONSISTENT INTERPRETATION, DIVERGENT APPLICATION AND LACK OF ACCEPTANCE OF THE EIDAS REGULATION IN RELATION TO QWACS (REGULATORY AND IMPLEMENTATION WEAKNESS)

Although the evaluation concluded that eIDAS has been successful in establishing an EU market for trust services, significant barriers remain for trust service providers, which hinder competition.

It is currently left to the discretion of supervisory bodies in each Member State how qualified trust service providers should be supervised. Furthermore, national conformity assessment bodies do not apply common standards in the conformity assessment of the qualified trust services and their providers. Nor is there a common approach on the scope and content of the conformity assessment reports issued as part of the assessment process[117]. According to the evaluation report about 50% of Member States have implemented procedures at national level for the qualification of Trust Service Providers (TSPs) however half of those procedures do not reference applicable standards. For the remaining Member States there is no public information or guidance to the criteria applied to a TSP, the required scope of the conformity assessment, and how and by whom it should be performed, whether there exists a review process by the national supervisory body, nor its content or duration[118].

Different national rules, non-harmonised applications, differences in fees[119] and certification periods create risks of forum-shopping. Choosing Member States where supervisory authorities and conformity assessment bodies may be more lenient in assessing the functional requirements of the regulation, negatively affects trust and confidence in qualified trust service providers.

A specific problem is connected to diverging national practices relates to remote identity verification. Remote identity verification is the process of validating a person's attributes and verifying if they really are

---

[114] Over 70% of Member States responding to a survey in the context of the eIDAS evaluation confirmed this.

[115] Effective identity matching is a key requirement for interoperability and access to services and a pre-condition for the seamless use of European Digital Identities, the absence of which prevents the opening up of services, extending the eIDAS Regulation to the private sector and the proper application of the Once-Only Principle at EU level (Article 14 of Regulation (EU) 2018/1724)

[116] The issue of identity matching is a strongly contributing factor to the poor performance of eIDAS notified eID in a cross-border context, and limits is usability. The eIDAS evaluation recommends e.g. to introduce a centralized repository for identity matching that would allow service providers perform the required identity matching automatically.

[117] Swedish Post and Telecom Authority's standpoint on eIDAS Regulation. (2020). (unpublished); Luxembourg Position on The Review of the Eidas Regulation. (2020). (unpublished).

[118] Different practices in conformity assessment have been criticised by the majority of Member States and stakeholders consulted on the eIDAS revision. In 2019, ENISA (see https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits) highlighted that the lack of a standardised approach to auditing TSPs was major shortcoming of the conformity assessment scheme. While providing that a conformity assessment report (CAR) should be produced and used by the Supervisory Body to determine the qualified status of TSPs, the eIDAS Regulation does not specify the form and depth of the analysis of a CAR. By leaving it to Supervisory Bodies to measure whether a TSP has reached the status of "qualified" or not, this seems to have resulted in “incongruences in the qualification of TSPs in different countries as well as their qualified trust services” with a negative impact on the trust service market and the associated risk of “Undermining trust and confidence in the quality of eIDAS-regulated QTSPs and services in the European Union.” (excerpt from the evaluation report)

[119] Audit costs can vary up to four times from one CAB to the other, for the same solution, depending on the severity of CABs’ approach

who they say they are without a physical face-to-face interaction. Such verification can instead be made through biometric identification or by verifying identity documents remote via video conference or video assisted automatic identification. Despite a common legal basis in the eIDAS Regulation which defines the circumstances for remote identification, there is a significant lack of harmonisation in applying these requirements across Member States:

Remote identification methods are currently left to the discretion of each Member State supervisory body, without any clear equivalence requirements applying to the physical presence mentioned in Article 24(1)(b)[120]. Consequently, the same remote identification methods can be accepted in some Member States and rejected in others.

As mentioned on page 16, the provision and use of website authentication services are entirely voluntary for web site owners. However, when web site owners choose to use QWACS, the browser must display information about its content to the user. Since the adoption of the eIDAS Regulation in 2014, web-browsers have not accepted the use of these certificates in the bowser environment, calling for additional regulatory intervention to ensure consumer choice.

As mentioned under problem 4 on page 16, the provision and use of website authentication services are entirely voluntary for web site owners. However, when web site owners choose to use QWACS, the browser must display information about its content to the user. Since the adoption of the eIDAS Regulation in 2014, web-browsers have not accepted the use of these certificates in the bowser environment, calling for additional regulatory intervention to ensure consumer choice.

2.3 HOW WILL THE PROBLEMS EVOLVE?

The evolution of the problems described should be seen in the light of expected trends on the identity market. Globally, an increase in demand for digital identity solutions is expected, with a predicted annual market growth ranging from 13%[121] to 20%[122]. In addition, it is likely that user expectations with regard to control of personal identity data[123] and effective technologies for fraud and identity theft prevention will continue to increase. Continued growth in mobile penetration strengthens the demand for convenient and secure mobile platforms and solutions[124]. Large private providers and online platforms are investing into providing secure identification, in particular for payment services[125]. The combination of convenient technological solutions and market power will in the medium term allow online platforms to offer secure identification for all use-cases, including public online services. This will increase the dependency of the larger players and continue to put political pressure on Member states to avoid the replacing of public eID and fear a de facto privatization of identification of physical persons in the digital world. Without promoting the use of legal identities requiring a high level of assurance linked to identity and identity attributes, the increased privatisation of digital identity and dependency on providers of social log-in Solutions are likely to continue with the inherent risk this poses to the security and privacy of identity data. The prominence of large players in an unregulated sector is also likely to challenge the competitiveness of European industry in this space. In the light of these expected trends, a no change scenario for the eIDAS Regulation may have the following impacts on the problems and drivers:

Not all EU citizens and businesses will have access to seamless user-centric trusted and secure digital identity solutions that can be conveniently used to authenticate to cross-border and cross-sector online services. In the absence of clear rules and incentives for private sector adoption of notified eIDs their usability will remain limited and users will not have the possibility to fully rely on the use of highly trustworthy solutions at the EU level empowering them. Only a few national eID solutions that are able to integrate private services and align with user preferences are likely to see continued growth in adoption at

[120] FESA. (2020). Position Paper On the review of the eIDAS Regulation FESA's answer to the European Commission's consultation.

[121] The Insight Partners. (2020). Europe Identity Verification Market to 2027

[122] Flood, G. (2019). Global Digital Identity Market to Hit $15BN By 2024. Think.Digital Partners. https://www.thinkdigitalpartners.com/news/2019/05/28/global-digital-identity-market-to-hit-15bn-by-2024/

[123] Eurobarometer 503 (Attitudes towards the impact of digitalisation on daily lives, December 2019): 63% of respondents want a secure single digital ID for all online services that gives them control over the use of their data, 72% of respondents want to know how their data are used when they use social media accounts.

[124] Deloitte. (2018). Trends in electronic identification: An overview - value proposition of eIDAS eID. European Commission. 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

[125] Google Pay, Apple Pay, Lybra

national level. Their cross-border use is unlikely to improve in the absence of regulatory change at EU level putting the functioning of the digital single market at risk. With regards to IoT devices, consumers will have to rely on a multitude of solutions, not relying on common rules for linking devices to a person in a reliable consumer controlled and secure digital environment. In the absence of a common solution for identity matching, cross-border usability of eIDs will remain limited and this would also pose a risk to the functioning of other EU legislation, such as the Once-Only Principle under the Single Digital Gateway Regulation.

Market fragmentation for private digital identity solutions is likely to grow in the absence of a unitary regulatory framework at EU level. It is likely that a few powerful players (e.g. online platforms), able to capitalise on technology and customer base, will take a large share of the digital identification market while smaller independent providers will see their market share reduced. This is likely to create dependencies for online service providers, user lock-in and a decrease in value creation as well as presenting a challenge to the EU's digital autonomy.

Users will not be able to control the use of their identity data in the absence of clear, uniform data protection and privacy safeguards for identity providers including online platforms. Online payment fraud is anticipated to grow[126]. Stakeholder trust, interoperability of trust services and further unequal market access are likely to suffer from a continuous inconsistent application of the regulation by supervisory authorities. Market fragmentation, growth below potential and limitations to international reach are other possible effects. A continuing refusal of web-browsers to support QWACs would leave the enforcement of consumer and privacy rights exclusively with supervisory bodies and transparency for citizen could not be ensured. On the contrary, a support of QWACs by web-browsers could create a competitive advantage for the security and transparency of online transactions in the EU**.**

On this background, the President and the European Council have called for a secure and trusted digital identity for all that protects data and can be used for public and private online services. This offer can only be attractive to the user if it includes the widest range of use-cases in one application – from highly sensitive eGovernment and eHealth applications to pseudonymous log-on options to online platforms. In addition, the offer must be as user-friendly as current platform solutions offering seamless user-journeys and short response times.

3 WHY SHOULD THE EU ACT?

This initiative aims to support Europe's digital transformation towards a Digital Single Market. With the growing digitization of public and private services accessible cross border relying on the use of digital identity solutions, there is a risk that citizens will continue to face obstacles and not make full use of online services easily and throughout the EU while preserving their privacy if left to Member States in accordance with the current legal framework. There is also the risk that the shortcomings of the current legal framework for trust services would increase fragmentation and reduce trust if left to Member States alone. Thus, Article 114 TFEU is identified as the relevant legal basis for this initiative.

3.1 SUBSIDIARITY: NECESSITY OF EU ACTION

Citizens and businesses should be able to benefit from the availability of highly secure and trustworthy digital identity solutions that can be used across the EU and the portability of electronic attestations of attributes linked to identity. Due to the current limitations of the eIDAS Regulation, in particular in view of recent technological developments, market and user demand, requiring the availability of more user friendly and true cross border solutions allowing access to online services EU wide. Users have also grown increasingly accustomed to globally available solutions, for example when accepting the use of Single Sign-On solutions provided by the larger social media platforms to access online services. Member States cannot alone address the challenges this creates in terms of privacy and market power of the large providers, which requires interoperability and trusted eIDs at the EU level In addition, electronic attestations of attributes issued and accepted in one Member State, like an electronic health certificate, is often not legally recognised and accepted in other Member States. This creates the risk that Member States continue to develop national solutions.

[126] 42.7 MEUR are expected to be spent on fraud detection and prevention software between 2017 and 2022. According to IBM Security and its '2018 Cost of Data Breach Study', the average total cost of a data breach, the average cost for each lost or stolen record (per capita cost), and the average size of data breaches are on the rise and expected to continue growing.

For the provision of Trust Services, although largely regulated and functioning in accordance with the current legal work, national practices also creates the risk of increased fragmentation. For example, video identification is recognised in some Member States while not in others and additional means of remote identification is made available on the market requiring a harmonised approach to avoid barriers. Furthermore, ensuring the use and acceptance of existing trust services cannot be done by Member States alone. For example, in the browser environment, ensuring the EU wide acceptance of Qualified Web Authentication Certificates has to be addressed at the EU level[127].

EU-level intervention is ultimately best suited to provide citizens and businesses the means to identify cross border and exchange personal identity attributes and credentials using highly secure and trustworthy digital identity solutions ensuring privacy. No single Member State can offer alternatives to solutions offered by large market players. This requires trusted and secure eID and a regulatory framework linking them to attributes and credentials at EU level. Only EU-level intervention can lay down the conditions that ensure user control and access to cross border online digital services and a interoperability framework making it easy for online services to rely on the use of digital identity solutions irrespective of where in the EU it has been issued or where a citizen resides. It is unlikely, as shown by the review of the eIDAS Regulation, that national intervention would be equally efficient and effective.

3.2 SUBSIDIARITY: ADDED VALUE OF EU ACTION

Considering the growing demand from citizens, businesses and providers of online services for user friendly, secure and privacy friendly digital identity solutions that can be used cross border, further action at the EU level can bring greater value than action by individual Member States, as shown by the evaluation of the eIDAS Regulation.

A more harmonised approach at the EU level based on the fundamental shift from the reliance on digital identity solutions alone to the provision of electronic attestations of attributes would ensure that citizens and businesses can have access to public and private services anywhere in the EU relying on verified proofs of identity and attributes. Online service providers would be able to accept digital identity solutions independently of where they have been issued, relying on a common European approach to trust, security and interoperability. Users and service providers alike can also benefit from the same legal value provided to electronic attestations of attributes across the EU, which is particularly important when coordinated action is necessary, like when it comes to digital health certificates. Trust services providing electronic attestations of attributes would also benefit from the availability of a European market for their services. For example, recuperating the costs to ensure a highly trustworthy and secure environment for the provision of Qualified Trust Service is more easily off-set at EU level due to economies of scale. Only an EU framework can ensure full cross-border portability of legal identities and electronic attestation of attributes linked to it making it possible to trust identity assertions made by other Member States.

Building on the current eIDAS framework for the provision of trust services, additional measures to further harmonise it would improve market conditions and ensure trust at the EU level. Moreover, the eIDAS regulation is setting the standards for trust services globally. To support the international competitiveness of European businesses it is necessary to ensure the regulatory framework for trust services remains relevant and effective. A more harmonised approach would also benefit Member States, ensuring compliance with obligations under EU and national law requiring that users identify to access services. For example, notified electronic identity solutions based on a common approach to identity matching will allow Member States to fulfil their obligations in accordance with the Single Digital Gateway Regulation. EU action would also provide users increased choice, not having to rely fully on the solutions provided by a handful of large online providers.

From the evaluation of the eIDAS Regulation, stakeholders largely agreed that the eIDAS Regulation has created added-value and is by many considered the most advanced framework in its field globally. The revised eIDAS Regulation will add further value addressing technological developments, user and market demands and make it unnecessary for businesses to develop own and sector-specific solutions.

The Conclusions of the European Council in October 2020 underpin the above and demonstrate Member States' agreement that national action alone would not suffice to reach the set objectives. Thus, the European

[127] In the 2017 Tallinn Declaration, Member States urged the Commission to take steps to increase the recognition of eIDAS compliant solutions by global market players, in particular for QWACs

Council stresses the need for action at European level, complementing the Commission's call for revising eIDAS in its Strategy on Shaping Europe's Digital Future and the commitment to deliver a secure European Digital Identity by the President of the Commission in her State of the Union Speech.

4 OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1 OVERARCHING OBJECTIVE

The overarching objective of the intervention is to ensure the proper functioning of the internal market, particularly in relation to the provision and use of cross-border and cross-sector public and private services relying on the availability and use of highly secure and trustworthy electronic identity solutions. Since the adoption of the eIDAS Regulation in 2014, and in particular since the Covid pandemic, which has accelerated the pace of digitalisation, meeting this objective has become imperative. There has been a significant increase in the importance of having secure digital identity solutions to identify and share verified electronic attributes and to rely on trust services such as e-signatures or seals, to allow citizens and businesses to provide and use digital services within and across borders, for personal, professional or health reasons.

In the Communication from the Commission "***2030 Digital Compass: the European way for the Digital Decade***[128]", the Commission has set out a number of targets, pursuing digital policies that empower people and businesses to seize a human centred, sustainable and prosperous digital future. Ensuring access to digital identities for all and enabling their use is identified as a key enabler to support many of the initiatives set out in this Communication. This includes the targets related to digitally enabled Health Services, secure and performant available infrastructures, digital transformation of businesses and of public services in particular. Reducing the need for travel and instead rely on the use of electronic identities, the provision of electronic attestations of attributes and electronic signatures and seals to access services and conclude agreements on a distance, the initiative is consistent with the European Green Deal initiative[129], transforming the EUs economy for a sustainable future.

4.2 OBJECTIVES

The objectives of the initiative seek to address the problems outlined in section 2 and reflect the political mandate formulated by the President of the Commission and by the European Council Conclusions.

OBJECTIVES FOR DIGITAL IDENTITY

PROVIDE ACCESS TO TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS THAT CAN BE USED CROSS BORDERS, MEETING USER EXPECTATIONS AND MARKET DEMAND

Achieving this objective would mean that the expectations users have to access seamless and trusted solutions to identify electronically and share electronic attestations of attributes cross-border can be met. Every EU citizen will have access to secure and user-friendly solutions for electronic identification that are capable of providing access to online public and private services in the EU. Fully achieving this objective will rely, not only on the capacity of Member States to issue eIDs to their citizens and to notify them, but also on new possibilities to be offered by private and public providers of secure and trustworthy identity data and attributes. This would also provide a practical and secure alternative to platform log-on services, while at the same time offering different levels of assurance and trust and the possibility to exchange the necessary data linked to identity for various public and private sector use-cases.

Achieving this objective would also allow EU digital industry compete at equal footing with large online platforms in the provision of digital identity solutions. EU digital industry would benefit from a rules-based link between identity attributes and credentials to trusted and secure eID provided by the public sector which would allow for the development of e.g. new independent e-commerce platforms and online services.

---

[128] (COM (2021) 118 final)

[129] (COM(2019) 640 final)

The drive for digital transformation instilled by the COVID context, the political commitment of the Member States expressed in the October Council Conclusions and the fact that most Member States are planning to use the Recovery and Resilience funds to reinforce their digital identities, on top of their digital transformation agendas, provides the confidence that time is ripe for a change.

This objective specifically responds to the following problem drivers "Notification by Member States of eID schemes under eIDAS is voluntary and the process is complex", "Market, societal and technological developments triggering new user and marked needs", "Not all Member States have notified national eID and opened them to the private sector for domestic reasons or for lack of incentives", "Private providers of digital identity attributes are not subject to a harmonised regulatory framework ensuring trust and security cross-border".

In bilateral exchanges with the Commission, many Member States have stressed the need to reinforce the eIDAS Regulation in order to accelerate the digital transformation and to adapt to a fundamentally changed global digital context.

ENSURE THAT PUBLIC AND PRIVATE SERVICES CAN RELY ON TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS CROSS BORDER

Responding to market and technological developments and evolving user needs, citizens and businesses would be offered the possibility to use eIDs issued in one Member State together with electronic attestation of attributes and credentials linked to their eID to access online public and private services across the EU, as well as other services relying on the use highly trustworthy digital identification solutions, for example when renting a bike or presenting a digital certificate required to cross a border. This would apply to online and offline services requiring users to identify with a high level of assurance and providing additional and trustworthy proofs in electronic forms (such as residence, place of birth, other identity credentials such as "student", "adulthood" / "seniorhood", etc.). For online service providers, it would mean that access to services no longer will have to be limited to citizens and businesses holding electronic identity solutions issued for specific sectors or a specific Member State. It would solve the problem of lack of uniformity, lack of identity data and interoperability preventing service providers from easily providing services requiring the use of secure and trust worthy digital identity solutions to all EU citizens.

In addition, online service providers would be able to rely on an impartial single-sign-on solution that protects business data and personal data covering all levels of assurance. This would offer service providers an alternative to identification solutions offered by large online platforms thus strengthening their independence and competitiveness.

Fully achieving this objective would require that all citizens and businesses have access to a notified eID and a mechanism to ensure that electronic attestations of attributes can be issued and provided to service providers requiring it. Fully achieving this objective will also require that regulated sectors are obliged to accept notified eIDs and electronic attestations of attributes and that the convenience of use and the level of trust provided by these solutions will encourage the wider uptake of eIDAS compatible electronic identity solutions in non-regulated sectors. Fully achieving this objective will also require that appropriate business models are found at the EU level.

This objective responds to the following drivers "Notification by Member States of eID schemes under eIDAS is voluntary and the process is complex", "Not all Member States have notified national eID and opened them to the private sector for domestic reasons or for lack of incentives", "Private providers of digital identity attributes are not subject to a harmonised regulatory framework ensuring trust and security cross-border", "Market, societal and technological developments triggering new user and market needs".

PROVIDE CITIZENS FULL CONTROL OF THEIR PERSONAL DATA AND ASSURE THEIR SECURITY WHEN USING DIGITAL IDENTITY SOLUTIONS".

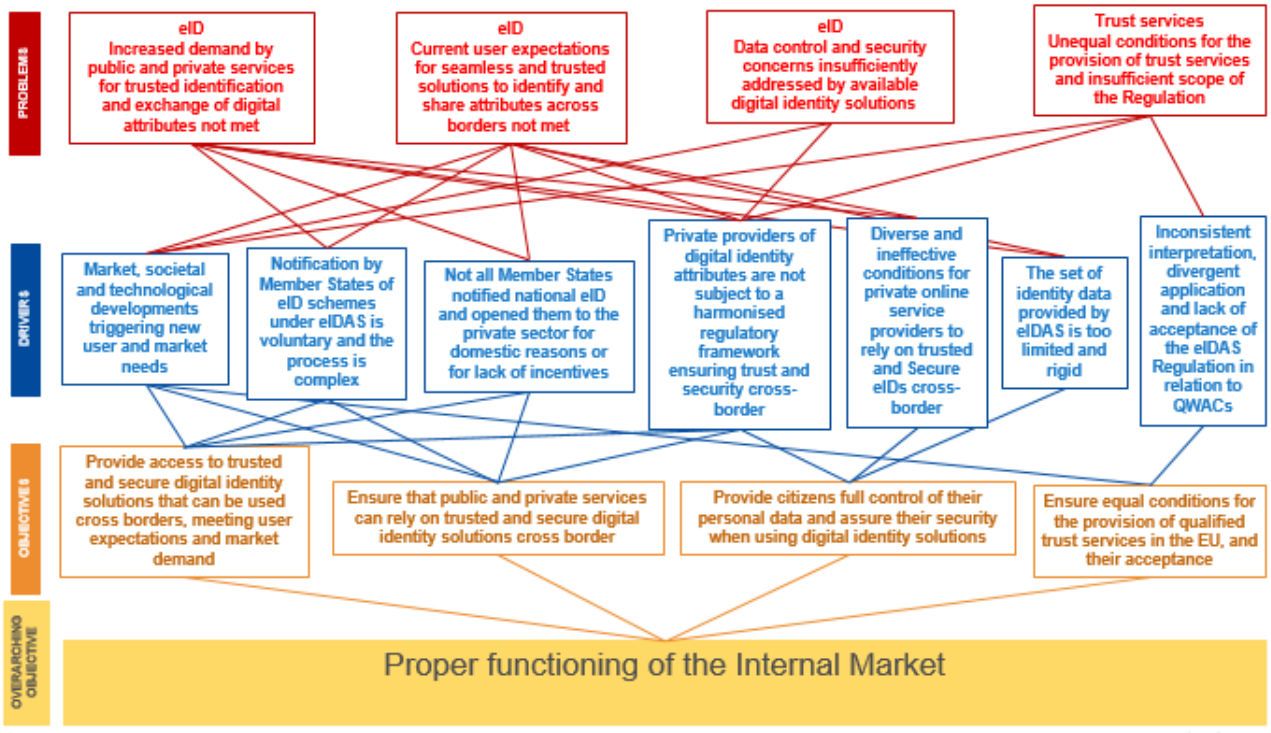
Achieving this objective would mean that users can manage and control their own identity data when using digital identity solutions. This will be done through trusted and secure government eID schemes and by the availability of a digital identity wallet and by using private qualified trust service providers of identity-related data and attributes. This objective responds to the following problem drivers: "Private providers of digital identity attributes are not subject to a harmonised regulatory framework that ensures their trust and security for cross-border use", "The set of identity data provided by eIDAS is too limited and rigid" and "Diverse and ineffective conditions for private online service providers to rely on trusted and secure eIDs cross-border".

OBJECTIVES FOR TRUST SERVICES

ENSURE EQUAL CONDITIONS FOR THE PROVISION OF QUALIFIED TRUST SERVICES IN THE EU AND THEIR ACCEPTANCE

Achieving this objective would mean that qualified trust service providers will be able to rely on fully harmonised rules across the EU for the provision of services, including the rules on remote identification, based on fully transparent procedures for the accreditation of trust service providers and a fully harmonised supervisory regime. Achieving this objective would also mean that the scope of the eIDAS Regulations covers all trust services requiring a common European approach, including the provision of qualified electronic archiving services. Achieving this objective would also mean that all qualified trust service can be relied upon by end-users. For example, that visitor to a website can rely upon Qualified Web Authentication Certificates made available in the browser environment, helping to protect against phishing attacks and fraud. This objective responds to the following drivers: "Market, societal and technological developments triggering new user and market needs" and "Inconsistent interpretations, divergent application and the lack of acceptance of the eIDAS Regulation in relation to Qualified Web Authentication Certificates".

Figure 5 - Problems, drivers and objectives



5 WHAT ARE THE AVAILABLE POLICY OPTIONS?

This section presents the policy options, including the baseline scenario, that have been considered for addressing the problems identified in chapter 2 and for meeting the objectives set out in chapter 4.

POLICY OPTIONS FOR EID:

The options presented below are based on a progressive interdependence and cumulative logic and design. They rely on different sets of measures reflecting gradual ambition levels. For instance, ***Option 2*** can only address all objectives if it builds on ***Option 1***, while ***Option 3*** only meets all of the objectives if it builds on measures under ***Option 1*** and ***Option 2***. The design of the options considered all possible political choices, at the level of all actions, aiming to address all problems and drivers as described above. When various intervention levels related to a certain action were possible, specific sub-options were put forward and explained.

The available options can be described as follows:

- ***Option 1 has a low ambition level*** and is based on a set of measures limited to preserve and strengthen the effectiveness and efficiency of the current eIDAS. By imposing mandatory notification of national eIDs and streamlining the existing instruments available to achieve mutual recognition, this option relies on the current philosophy of eIDAS: meeting citizens' needs by relying on diverse government national e-ID schemes that aim to become interoperable.

⇨ ***Interdependencies*** with other options: By strengthening the national notified eIDs, option 1 provides the building blocks needed to implement Options 2 and 3, since they both need to rely on the trust anchor provided by the notified eIDs.

- ***Option 2 has a medium ambition level*** which mainly aims to extend the scope of the current framework by establishing a fully-fledged ecosystem for the secure exchange of potentially any data linked to identity, particularly to accommodate the private sector demand for such data (beyond government eIDs and not replacing but complementing them) supporting the current shift towards attribute based identity services. The aim is to meet part of citizens' new demands by the secure provision of attributes and credentials such as a proof of being above 18 or certificate of a professional degree. This would be achieved by the creation of a new trust service enabling qualified trust service providers to offer credentials and attributes linked to trusted sources and therefore enforceable across borders. To identify the person to whom the identity data is linked, trust service providers will need to link the attributes and credentials to the notified eIDs of the users. This option marks a change from the current eIDAS philosophy, designed with the initial aim to exclusively support the public sector use cases by the use of diverse interoperable government eIDs. ***Option 2*** would extend the scope of the Regulation by empowering the European citizens and companies to use and exchange any data linked to identity (attributes) in the widest range of use cases possible, in all their public and private transactions.

  ⇨ **Interdependencies** with other options: as the new trust service needs to rely on notified eIDs, ***Option 2*** is cumulative, as it cannot address all the objectives unless it builds on most of the measures in ***Option 1***.

- ***Option 3 has a high ambition level*** and regulates the provision, as a qualified trust service (under Sub-option 1), or by Member States (under Sub-Option 2), of a personal digital wallet allowing citizens to store and manage identity data and electronic attestations of attributes securely on their devices. With the wallet, the user will be able to authenticate and identify him/herself to access services online or to prove data related to him/herself. The wallet would be able to store and exchange the information provided either by governments under their notified eIDs (e.g. name, surname, date of birth, nationality, which would testify, for instance, the right to reside, to work, or to study in a certain Member State) or by trust service providers described under ***Option 2*** (e.g. attributes and credentials such as professional qualifications, employment history or credit worthiness which could support users, for instance, to get a new job or a loan). Apart from convenience of use, the wallet will allow for the easy selective disclosure of the identity data. In the same way bank cards are used today to authorise payments, digital wallets will authorise the release of trusted information about users to third parties, under their full control.

  Option 3 also implies a change in paradigm when compared to the baseline. To ensure seamless interoperability, security and full data-control in a user-friendly environment, a common technical architecture and reference framework and common standards would be developed. It will therefore no longer be necessary to rely on the eIDAS technical nodes, reducing implementation time and rendering the system more resilient and adaptive to technological change and to evolving user needs and convenience expectations. In order to guarantee trustworthiness across borders, ***the wallets will be linked to the eIDs of the users notified by all Member States, as described under Option 1.***

  ⇨ ***Interdependencies*** with other options: ***Option 3*** is cumulative as it only meets all the objectives if it builds on measures under ***Option 1*** (the wallet needs to be linked to a notified eID) and on the measures put forward under ***Option 2*** (attributes issued by the new qualified trust service providers need to be compatible with and integrated in the wallet).

IN RELATION TO TRUST SERVICES:

The 3 options build on the same level of ambition and rely on a similar set of measures. Since most of the inefficiencies triggered by the lack of harmonisation can be solved under the baseline, which also covers the soft level measures, the remaining objective to meet the demand for new trust services can be implemented only via legislative intervention. Since no intermediate level of intervention has been identified when compared to the baseline, all 3 options are put forward to rely on the same set of measures.

Figure 6 - Overview of policy options

Policy objectives	**POLICY OPTIONS**			
	PO 0 (baseline)	**PO1** (legislative) **Improve the current legal framework for cross-border recognition of national eIDs and trust services**	**PO2** (legislative) **Creating a market for the secure exchange of Data linked to Identity**	**PO3** (legislative) PREFERRED OPTION **Personal digital identity wallet (EUeID)**
O1: Provide access to trusted and secure digital identity solutions that can be used cross borders, meeting user expectations and market demand	No change in scope of eIDAS (eID + current set of trust services), requirements (mutual recognition, supervision) and obligations (voluntary notification)	**M1:1** Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure.	**M1:1** Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure. **M2:1** Create a new Qualified Trust service for the secure exchange of data linked to identity. **M2:2** Require MS to make available data stored in authentic sources for the secure exchange of data linked to identity.	**M1:1** Establish an obligation for MS to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure. **M2:1** Creating a new Qualified Trust service for secure exchange of data linked to identity. **M2:2** Require MS to make available data stored in authentic sources for the secure exchange of data linked to identity. **M3:1 (SUB-OPTION 1)**: Creating a new qualified trust service for the provision of a user-controlled secure European Digital Identity WalletApp. **M3:1 (SUB-OPTION 2):** Extension of notified eID schemes or provision of a user-controlled secure European Digital Identity WalletApp by MS.
O2: Ensure that public and private services can rely on trusted and secure digital identity solutions cross border	Under the DMA, gatekeepers will be required, under certain circumstances, to offer access and interoperability with notified eIDs	**M1:2** Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs **M1:3** Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs **M1:4** Extend the person identification data set recognised cross border	**M1:4** Extend the person identification data set recognised cross border **M2:3** Setting security requirements and common technical standards for the secure exchange of data linked to identity. **M2:4** Define the legal effect of digital identity credentials **M2:5** Regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials	**M1:4** Extend the person identification data set recognised cross border **M2:3** Setting security requirements and common technical standards for the secure exchange of data linked to identity. **M2:4** Define the legal effect of digital identity credentials **M2:5** Regulated sectors such as energy or finance and the Public Sector would be required to rely on Qualified digital credentials **M3:2** Defining common standards for a European Digital Identity Wallet App

				M3:3 Security requirements
O4: Provide citizens full control of their personal data and assure their security when using digital identity solutions	Require MS to limit identification data transmission to only the data necessary for a particular transaction.	**M1:5** Strengthen security requirements for mutual recognition	**M1:5** Strengthen security requirements for mutual recognition **M2:6** Legal requirements to ensure the protection of personal data	**M1:5** Strengthen security requirements for mutual recognition **M2:6** Legal requirements on trust service providers of data linked to identity to ensure the protection of personal data
O5: Ensure equal conditions for the provision of qualified trust services in the EU, and their acceptance	Harmonise Supervisory Procedures for Trust Services Measures to streamline peer-reviews and the cooperation mechanisms between Member States	**M1:6** Introducing a new trust service for eArchiving **M1:7** Harmonise the certification process for remote electronic signing **M1:8** Strengthening the recognition of Qualified Website Authentication Certificates (QWACS)	**M1:6** Introducing a new trust service for eArchiving **M1:7** Harmonise the certification process for remote electronic signing **M1:8** Strengthening the recognition of Qualified Website Authentication Certificates (QWACS)	**M1:6** Introducing a new trust service for eArchiving **M1:7** Harmonise the certification process for remote electronic signing **M1:8** Strengthening the recognition of Qualified Website Authentication Certificates (QWACS)

WHAT IS THE BASELINE FROM WHICH THE POLICY OPTIONS WILL BE ASSESSED?

Under the baseline scenario, the Commission would not propose to change the eIDAS Regulation. The baseline would integrate measures envisaged under secondary legislation that could be enforced without any changes brought to the Regulation (implementing acts foreseen in the Regulation but not yet adopted) or implementing acts which were adopted and which could be potentially amended to further optimize the system. Similarly, positive spill-overs stemming from other pieces of legislation (e.g. Digital Markets Act) would be considered under the baseline. Most Member States agree on the benefits from further harmonising certain aspects of the eIDAS Regulation via the use of secondary legislation available under the baseline (i.e. implementing acts).

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

Improvements would also be sought by upgrading most of the ***soft-law instruments***. However, even updating certain existing guidelines without an enabling legislative change in the Regulation might be difficult given the current conflicting positions by Member States on issues such as remote identity proofing or the delineation between levels of assurance in relation to certain technologies.

Generally, under the baseline scenario, it is expected that the weaknesses of the current legal framework, as identified by the eIDAS evaluation will persist and even amplify. The ambition to provide all EU citizens with a trusted and secure identity enabling access to a wide range of public and private cross-border digital services and with control over identity data would not be achieved.

As reflected in the problem definition section, the current deficiencies of the eID system go beyond absence of notifications. Even if the pace of notifications would accelerate under the baseline and all Member States notify at least one eID scheme, it is generally expected that the complexity brought by the interaction of 27 notified schemes would amplify the systemic deficiencies, as identified by the eIDAS evaluation, to an even larger scale. Notifications would not address the issue of limited access to public and private services in the Union and would not empower citizens to fully dispose of their digital identity data in all their public and private transactions. It should be acknowledged, however that notified eIDs would play a crucial role in a new digital identity ecosystem built on commonly agreed standards, to be further detailed under the description of the options section.

Consequently, the baseline would not provide the tools needed to fill the current gaps raised by the increasing demand for cross-border use of data linked to identity (attributes) and the convenience, versatility and the security needed to manage these attributes.

With respect to the relevant measures that could be taken in relation to ***electronic identification***, amending the eIDAS technical specifications could potentially remove the current rigidity in the transmission of the data-set (e.g. the whole data-set transmitted by default) and integrate concepts such as data minimisation and zero-knowledge claims. The baseline would require public authorities to implement technical adaptations in the attempt to limit the identity data transmission via the notified eIDs to the minimum required for a specific transaction. Thus it could make a step in the right direction and allow citizens to take more control of their identity data and facilitate closer alignment with the European General Data Protection Regulation.

Similarly, as part of the baseline, certain actions could produce positive effects by amending existing implementing acts for eID with the aim to facilitate Member States' journey through the notification process. For instance, a smoother peer review process and better cooperation mechanisms between Member States could be explored[130].

As part of the baseline scenario, providers of core platform services that are designated as ***gatekeepers*** would be obliged to offer access to and interoperability with the same operating system, hardware or software

[130] Amendment of COMMISSION IMPLEMENTING DECISION (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification or COMMISSION IMPLEMENTING DECISION (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification

features under equal conditions for alternative providers of eID solutions, e.g. national eID notified under eIDAS. Designated gatekeepers will additionally be required to allow alternative applications access to their mobile infrastructure. While these obligations will give business users of core platform services the possibility to use electronic identity solutions other than those provided by the gatekeepers, it falls short of ensuring that citizens can directly rely on notified eIDs to access gatekeeper services or online platforms in general. Requiring gatekeepers to offer access and interoperability with notified eIDs would aim to increase citizens' security online and user control and trust in notified eIDs. Citizens and end-users would be enabled to use notified eIDs more widely and to provide only the minimum required data related to attributes specific to any transaction. The implementation of these requirements would however rely on the obligation for designated gatekeepers proposed by the Commission under the Digital Markets Act draft Regulation to materialise[131]. However, not all providers of core platform services would be covered by the DMA obligation.

Standards also carry the potential to improve the baseline scenario and provide a reference for providers to prove compliance with the requirements of the Regulation. The lack of relevant standards has already affected the mutual recognition of eIDs particularly in relation to the levels of assurance of mobile eID schemes, which has led to disagreements in the past. (e.g. the notification of a scheme at level "high" while the Cooperation Network adopted an opinion at level "substantial").

Assuming that eIDAS remains unchanged, ***new technologies and market based solutions*** might cover certain emerging user needs. However, in relation to those transactions requiring full certainty on the identity of the users (e.g. as required by law), this can be currently offered exclusively by relying on the state-sponsored identity schemes. In addition, these private identity solutions would operate without any recognised legal effect cross-borders since they are currently outside the scope of eIDAS Regulation. Since there are no objective references for users and businesses against which to assess their level of security, these solutions will be more prone to fraud and cybersecurity threats.

As far as ***citizens needs*** are concerned, it is expected that under the baseline they will increasingly expect digital identity solutions capable to manage, for instance, the hundreds of passwords used today when authenticating online and to have their identity data protected at all times. The need for digital identity solutions that can be self-managed and where, beside passwords, any other identity data or credentials can be stored, is expected to grow. For instance, all these elements are behind the rapid increase and growing adoption of digital wallets, both in the public and private sector.

In the light of the above, it is therefore expected that the underlying problems linked to the current mutual recognition based system to subsist and even amplify. As reflected by the problem definition, the current deficiencies linked to electronic identification go beyond mere implementation issues. As the implementing acts referenced in the eID part of the Regulation have been already adopted, there is no further margin for improvement via legislative intervention.

Under the baseline scenario, the scope of the legislation would remain limited to notified eID schemes, enabling access to online public services, however leaving the largest part of the digital identity related transactions outside the scope of eIDAS. Indeed, most of the demand for electronic identity and remote authentication stems from the private sector, particularly in areas such as finance, health, insurance, telecom or platform operators that are required by law to verify the identity of their customers.

The following inherent deficiencies of the current ecosystem are expected to subsist and even amplify:

- Member States would continue to notify national eID schemes on a ***voluntary basis***. As the notification process is what ensures mutual recognition of eID schemes across the EU, only the citizens of those Member States that chose to notify a scheme would be able to use eID in a cross-border context, while citizens of Member States that have not notified would still be deprived of this possibility. Even in a scenario where all Member States notify, the systemic shortcomings of a mutual recognition-based system will persist and possibly grow in scale as the interoperability system gains complexity.

[131] In accordance with Article 6(f)127 gatekeepers should allow providers of ancillary services (which includes identity services) access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeepers of such ancillary services.

- The overall ***user experience*** and cross-border authentication through eIDAS under the baseline scenario is expected to remain unattractive for end users, who will continue to face difficulties when trying to access public services in another country. In addition, citizens will continue to face obstacles when trying to use their secure eIDs to access online services provided by the private sector.
- It is also likely that the ***number of public services*** connected to the eIDAS network will grow slowly depending on Member States integrating eGovernment services on central platforms or gateways (as deployed, for instance, in Estonia) and addressing other blocking factors such as identity matching. Citizens' access to services will continue to depend on technical and architectural choices made by Member States on their national identity systems.
- The ***limited data-set of eIDAS*** would continue to be a barrier to supporting the specific needs of the private sector (e.g. health, banking, etc.) and to solving identity matching problems. As a result the possible use-cases under eIDAS would continue to be limited.
- Access of ***private sector*** service providers to trusted and secure eID is likely to remain limited. Even if all notifying Member States open their eIDAS nodes to private sector services cross-border, the diversity of national conditions for the use of eID infrastructures will still make it very difficult for service providers to build a sustainable business case. Private service provider access to notified eID schemes would likely continue to be scattered and remain mostly at domestic level.
- Overall in the light of these difficulties, it is expected that the ***number of cross-border authentications*** with trusted and secure eID will remain low, particularly when compared to the usage of eIDs at national level, and it is likely that private solutions will gradually replace public eID once they can offer similar assurance levels.

In general, it is expected that the rapid evolution of technologies will disrupt the current market for digital identity and authentication solutions. Single-Sign-On solutions and digital platforms and wallets able to manage a variety of identity data and credentials that can be easily stored and presented to service providers are likely to proliferate. The global COVID-19 pandemic will undoubtedly accelerate the trend for convenient and secure identification to essential public (eHealth) and private services (e.g. banking).

In relation to ***trust services***, the inconsistent interpretation and application of rules for trust services could be alleviated by the adoption of the implementing acts currently referenced under the Regulation aiming to further harmonise the supervisory procedures in the Member States. The harmonisation of supervisory procedures for trust services would require public authorities to actively participate in the shaping of the implementing acts and to ensure a better coordination with their peers in other Member States after their adoption

The adoption of implementing acts and referencing standards have the potential to reduce the current fragmentation in relation to the certification of qualified trust service providers and the supervision systems established in Member States. However, remedy measures to address the emergence of new services or the non-recognition of qualified website certificates (QWACs) by web-browsers would not be possible under the baseline scenario since they would require changes to the Regulation. The baseline would also not include an extension to new trust services (e.g. eArchiving).

5.1 POLICY OPTION 1- LOW LEVEL AMBITION INTERVENTION: IMPROVE THE CURRENT LEGAL FRAMEWORK FOR CROSS-BORDER RECOGNITION OF NATIONAL EIDS AND TRUST SERVICES

This Option relies on a strengthened and streamlined legislative framework for national eIDs notified under eIDAS. It would require Member States to make eIDs available to all citizens and companies for cross-border use and focus on improving the effectiveness and efficiency of the current mutual recognition enabling instruments (e.g. peer-reviews, notifications). The use of national eIDs by private online service providers would be facilitated by measures aiming to establish, for instance, harmonised cost and liability models, extended data sets or access obligations for the Member States. All these measures would be taken without extending the scope of the eIDAS Regulation nor affecting its underlying principle: e.g. mutual recognition of diverse eID schemes based on different standards.

The intervention under ***Option 1*** would be supported by the following core measures:

MEASURE TO PROVIDE ACCESS TO TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS THAT CAN BE USED CROSS BORDERS, MEETING USER EXPECTATIONS AND MARKET DEMAND

MEASURE 1: ESTABLISH AN OBLIGATION FOR MEMBER STATES TO OFFER EIDS AND TO NOTIFY THEM UNDER EIDAS, FACILITATED BY A STREAMLINED NOTIFICATION PROCEDURE

This measure would imply an amendment of the ***Regulation*** establishing an ***obligation*** for the Member States both to provide their citizens and companies with electronic identification means (e.g. eID cards, mobile apps), and to notify them under national schemes in line with the eIDAS rules. The measure would also set clear mandatory deadlines for the submission of notifications and for the peer reviews to be carried out on the notified schemes.

In addition, this measure would streamline the current notification procedures by shortening the time from the pre-notification of an eID scheme until it can be legally used by citizens and businesses to access online public services cross border . The aim is to make the notification process more efficient and effective.

MEASURES TO ENSURE THAT PUBLIC AND PRIVATE SERVICES CAN RELY ON TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS CROSS BORDER

MEASURE 2: ESTABLISH A REQUIREMENT FOR MEMBER STATES TO ALLOW PRIVATE ONLINE SERVICE PROVIDERS ACROSS THE EU TO RELY ON NOTIFIED EIDS

This measure aims to increase the private sector use of notified eIDs by establishing a requirement in the Regulation for Member States to allow the use of the eIDAS network and of their notified eID schemes to online service providers[132]. For this to function in a cross-border context, prior agreement as regards the conditions for access to the eIDAS node will be necessary between the service provider and the identity provider in the concerned Member States (the measure implies amending the Regulation).

Example: A bank in *Member* State Y would be able to digitally register clients from Member State X via the national eID and the eIDAS node of Member State X. The eIDAS node would be by default open for cross-border use by private relying parties.

MEASURE 3: ESTABLISH A HARMONISED COST-MODEL AND LIABILITY RULES TO FACILITATE PRIVATE ONLINE SERVICE PROVIDERS TO RELY ON NOTIFIED EIDS

The goal of this measure is to establish a commercial model for the eIDAS network which clarifies the possible business relationships between Member States offering access to their national eID schemes and to the eIDAS network and the private online service providers wishing to use the identification possibilities provided by notified eID schemes for their own commercial purposes[133].

Currently, the landscape is extremely diverse. Some Member States allow the reuse of at least one eID scheme by domestic private relying parties for national transactions. Other Member States even envisage to open this possibility to private relying parties established outside their national territory. Some Member States are not allowing the reuse of their national eID schemes by private relying parties at the national level and are unlikely to do so for private relying parties established outside their territory.

The commercial model would establish the cost model for the private online service providers to access the eIDAS network[134], the contractual conditions between the service provider and the identity provider in the eIDAS network, and the respective security requirements. The existing eIDAS eID technical specifications would need to be adapted accordingly to accommodate all these dimensions.

The commercial contract model would be complemented by additional ***liability rules in the eIDAS Regulation*** applicable to all parties participating in the ecosystem (e.g. the notifying Member- State, the party issuing the electronic identification means, the party operating the authentication procedure) for possible damages due to failure in complying with the eIDAS rules (the measure would imply the amendment of the Regulation and related implementing legislation).

---

[132] Currently, Member States have full discretion to decide the approach in relation to the possibility for private service providers to rely on national eIDs. In Netherlands, for instance, Digi D is open only to organisations with a public mission. This might raise difficulties for the Member States to agree on a harmonized approach

[133] The commercial model would clarify the nature of the identity–related products and services ("What"), the different types of stakeholders involved in the ecosystem and their roles ("to whom") and the way these identity products/services will be delivered, in terms of operating model, cost, pricing and billing strategy ("how").

[134] Currently, relying on an eID system to access public services is free of charge. The conditions for private online service providers to access the eIDAS nodes, pricing and billing, are currently established only at national level and Member States' approaches vary (from free access to detailed charging models).

Example: A car rental company in country X would be able to rely on the notified eID of a customer in country Y to conclude a transaction since clear terms and conditions would be in place related to the eIDAS node the company would need to connect.

MEASURE 4: EXTEND THE PERSON IDENTIFICATION DATA SET RECOGNISED CROSS BORDER

In order to support a larger ecosystem of use cases, particularly in the private sector, this measure would rely on an amendment of the Regulation in order to support the ***design, definition and addition*** to the current eIDAS minimum data-set of other attributes and related data-sets necessary to access certain sector-specific services. In addition, the mandatory data-set uniquely representing a natural or a legal person would be extended with a fully persistent eIDAS identifier accepted at European level whose expression would be defined in full agreement by the Member States[135]. The eIDAS technical specifications would be amended to support additional services relying on these additional attributes. This measure received substantial support from Member States, as reflected in the position paper put forward by the Forum of European Supervisory Trust Service Providers. Stakeholder feedback from the interviews conducted as part of preparing this impact assessment also show general support for extending the minimum data set.

This persistent identifier and the additional attributes would considerably facilitate the comparison/matching of various identities of the same person, issued in various contexts or by different Member States (record matching / identity matching) which currently hinders citizens' effective authentication and access to services. To this end, the characteristics and persistency of the ***unique identifier*** already in use the eIDAS framework will be reviewed and improved to support more secure and unique record/identity matching. This unique identifier could be built on existing national identifiers linked for the specific purpose of the European Digital Identity without prejudice to the sovereign responsibility of Member States to determine how to ensure the uniqueness of legal identities. Full assurance on record matching / identity matching is a precondition for a seamless cross-border functioning of a European Digital Identity for persons, companies and devices[136].

Example: Personal attributes such as the current address (relevant, for instance, for the delivery of certain types of services) or nationality could be used by citizens in their online transactions once Member States agree on this data to become mandatory as part of the minimum data set[137]. An extension of the current minimum data set to data relevant for the provision and exchange of digital certificates in the health sector could enable EU-wide secure access to such certificates for medical tests or other health purposes.

MEASURE TO PROVIDE CITIZENS FULL CONTROL OF THEIR PERSONAL DATA AND ASSURE THEIR SECURITY WHEN USING DIGITAL IDENTITY SOLUTIONS

MEASURE 5: STRENGTHEN SECURITY REQUIREMENTS FOR MUTUAL RECOGNITION

In order to build trust in the cross-border use of notified eID schemes, the notifying Member State needs to demonstrate how the notified eID scheme fulfils the interoperability and security requirements provided by the eIDAS Regulation and relevant implementing acts.

One of the targeted actions would be to open the possibility for Member States to make use, in the notification processes, of conformity assessment bodies and reports to assess how their eID schemes meet the legal requirements. With regard to ICT security, Member States would also be able to use the voluntary ***certification*** schemes to be established at EU level – e.g. the future common criteria certification scheme (EUCC [138] scheme), or a targeted certification for specific elements of the eID schemes under the

[135] Currently, the unique identifier should be "as persistent as possible " and it can vary since it is constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification, with the aim of being as persistent as possible in time.

[136] The issue of identity matching is a strongly contributing factor to the poor performance of eIDAS notified eID in a cross-border context, and limits is usability. The eIDAS evaluation recommends e.g. to introduce a centralized repository for identity matching that would allow service providers perform the required identity matching automatically.

[137] The notion of minimum data set is linked to GDPR requirements and obligations. Any additional data will have to be provided only whenever needed and with the explicit consent of the user. This mean that such additional data will have to be made available at the request of the owner of the eID means.

[138] Common Criteria based European candidate cybersecurity certification scheme successor to the existing schemes operating under the SOG-IS MRA. The scheme looks into the certification of ICT products cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045.

Cybersecurity Act (combination of Article 54 and 47.5[139]). Currently, the cybersecurity certification of ICT products, ICT services and ICT processes is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven scheme[140]. The possibility to use certification schemes could be referenced as ways to prove compliance with security and interoperability requirements, such as the capacity of the eID schemes to resist against attackers with high attack potential as set in the Implementing act 2015/1502.

Objective security standards, conformity assessment reports and ICT security certification could reduce divergences between Member States on the security-merits of certain eID solutions and technologies. This could particularly facilitate the deployment of mobile solutions and eID solutions based on remote on-boarding or biometric authentication where security features are often under debate linked to the absence of clear boundaries between levels "substantial" and "high".

In addition, a formal process could be established to monitor and ensure that security functionalities and cryptographic algorithms of notified eID schemes are updated on a regular basis to uphold the security of the electronic identification means. This is already in place for trust services (audits, regular revisions of standards, etc.).

Option 1 relies on the data protection measures considered as part of the baseline scenario.

Example: Certification of eID means at EU level could be used to prove compliance with the security requirements for a mobile eID scheme assessed against level "High" in respect to its capacity to resist *against attackers with high attack potential*.

MEASURES TO ENSURE EQUAL CONDITIONS FOR THE PROVISION OF QUALIFIED TRUST SERVICES IN THE EU AND THEIR ACCEPTANCE

MEASURE 6: INTRODUCING NEW TRUST SERVICES

This measure will expand the scope of the eIDAS Regulation and add a ***new trust service*** for e-archiving[141] setting out common requirements and reference standards for the preservation of electronic documents. This will reduce fragmentation at the European level and provide a common market for trust services providing eArchiving services in the EU[142].

MEASURE 7: HARMONISE THE CERTIFICATION PROCESS FOR REMOTE ELECTRONIC SIGNING

This measure would rely on the empowerment in the eIDAS Regulation to amend CID (UE) 2016/650[143] and reference the available standards for qualified electronic signature and seals creation devices allowing qualified trust service providers to manage electronic signature creation data on behalf of their customers.

MEASURE 8: STRENGTHENING THE RECOGNITION OF QWACS (QUALIFIED WEBSITE AUTHENTICATION CERTIFICATES)

In order to improve the recognition of QWACs by web-browsers, a specific provision in the Regulation requiring web-browsers to ensure support and interoperability with QWACs would need to be introduced. This would require web-browsers to recognise QWACs and display the identity data these certificates provide. This would allow web-site owners to assert identity of a website and users to know who is behind it with a high degree of certainty. An implementing act will reference the standards and define these requirements in more detail.

---

[139] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices, protecting the right of consumers to know the legal entities they are interacting with, their geographical location to the point that providing misleading/inaccurate information or no information at all on the true identity of the business/trader, amounts to misleading or aggressive commercial practice (and fall short of consumer fraud).

[140] Cybersecurity Act, Recital 67.

[141] Electronic archiving aims at ensuring that a document is stored in order to guarantee its integrity (and other legal features). The technology underpinning electronic archiving therefore targets the document. Under the current eIDAS, electronic archiving remains the competence of Member States, to be regulated as a trust service in the future.

[142] 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 does not specify requirements and which standards should be used. Several stakeholders have mentioned that eArchiving should be added to the list of trust services.

[143] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 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 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. The Commission is currently engaged in an advanced dialogue with the Member States to amend the implementing decision

5.2 POLICY OPTION 2 - MEDIUM LEVEL AMBITION INTERVENTION: CREATING A MARKET FOR THE SECURE EXCHANGE OF DATA LINKED TO IDENTITY

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

In line with the eIDAS rules on trust services, the revised regulation would create ***a new qualified trust service*** (QTS) for the electronic attestation of attributes verified against authentic sources. Market players active in this area not wishing to become qualified providers of electronic attestations of attributes (***non-qualified trust service providers)*** will be subject to less stringent rules (For example, Measure 6 on the protection of personal data would only partially apply to them).

Option 2 is built on the following specific measures:

MEASURES TO PROVIDE ACCESS TO TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS THAT CAN BE USED CROSS BORDERS, MEETING USER EXPECTATIONS AND MARKET DEMAND

MEASURE 1: CREATING A NEW QUALIFIED TRUST SERVICE FOR THE SECURE EXCHANGE OF DATA LINKED TO IDENTITY

Based on the current eIDAS framework for the provision of qualified trust services, this service would be subject to common rules, equally applicable in all Member States, in order to ensure security, transparency, auditability and recognition across borders. It would organise the provision and exchange of attributes related to identity, such as name, address and age, medical certificates or other types of information linked to a person such as a professional qualifications or a digital driver's licence. These attributes would be asserted by credentials provided by public and private entities who hold the relevant data-sources or have access to them under a legal and technical framework. To ensure the cross-border legal effect of these credentials and their trustworthiness, they would need to be linked to national eIDs / eID credentials provided by Member States for their citizens and residents, and verified by the provider of the attributes. The service would therefore be only available to citizens from those Member States that have notified national eIDs under eIDAS. These credentials linked to national eID could then be used by physical and legal persons to identify or authenticate themselves online or to get an authorisation. The feedback received from Member States show support for the need to establish a trust service allowing for the widespread use of electronic attributes in the private sector. Also the private sector considers, based on the feedback received as part of the various consultation activities for this impacts assessment, that introducing a new trust service for the provision of attributes is essential to support multiple use cases related to online and offline transactions.

The following typical use cases linked to this new trust service for the secure exchange of data linked to identity can be identified:

Exchanging digital credentials**:** By sharing a digital credential, a user may demonstrate ownership of a valid driving licence when renting a car, prove his/her medical test to a doctor or confirm a medical degree at cross border level. A qualified trust service provider with prior user consent will access the data source and provide these credentials to the user thus allowing their exchange.

Accessing financial services in another Member State. By proof of identity and delivery of a pre-existing Customer Due Diligence record[144] a person could immediately engage in a financial relationship such as opening a bank account in another country[145].

[144] Know your customer (KYC) guidelines in financial services require verifying the identity, suitability, and risks involved with maintaining a client relationship and fit within the broader scope of anti-money laundering policy.

[145] This assumes harmonization of anti-money laundering and regulatory approval of such processes

Asserting specific attributes (e.g. proof of age, proof of residence, proof of establishment in a country): a user wishes to confirm his/her age to access a specific online service, download age-restricted content or buy alcohol without having to release any other personal information such as name or birth-date. At the request of the user, a qualified trust service provider provides credentials asserting these attributes based on data from relevant authentic sources, thus allowing the user to confirm personal characteristics in an anonymous trustworthy certified way.

As for all other qualified trust services under eIDAS, qualified trust service providers offering secure exchange of data linked to identity will be obliged to ***verify the identity of the natural or legal person*** to whom the service is provided. In the case of this new trust service, the qualified trust service provider will be obliged to ***rely on national eIDs notified by Member States***. The trust service provider will also need to make sure data can be securely shared with the relying party.

Digital credentials shared under the sole control of the user can be used for purposes of identification or authentication / authorisation, including in relation to IoT devices ensuring that a device is linked to the identity of a person to cover specific use cases.

Whenever the use of legal identities is required by law, for example to identify and authenticate to access an online service of a national tax authority, electronic attestations of attributes linked to the identity cannot substitute the legal identities issued by Member States for online identification[146].

In accordance with the rules already applicable to other qualified trust services under eIDAS, qualified providers of trust services for the secure exchange of data would benefit from a ***supervisory regime*** based on supervision, common rules for accreditation, security and liability underpinned by commonly agreed technical standards.

MEASURE 2: REQUIRE MEMBER STATES TO MAKE AVAILABLE DATA STORED IN AUTHENTIC SOURCES FOR THE SECURE EXCHANGE OF DATA LINKED TO IDENTITY

Member States would be required, under the full control of the user or data subject, to allow qualified trust services access to the identity data stored in authentic sources required for the specific service[147]. This requires a technical and legal link between the trust service providers and these authentic sources. Member States would need to make available data stored in authentic sources (public registers and databases). The capacity to verify attributes against trusted sources would be a pre-requisite for the provision of services by qualified providers of trust services for the secure exchange of electronic attestations of attributes. However, this measure would not impose an obligation on Member States to offer full access to national registries, but exclusively restricted to what is required for the service in question. Qualified service providers would only be allowed to query specific data from national registries via standardised Application Programming Interfaces (APIs) with prior consent of and mandate from the user[148].

MEASURES TO ENSURE THAT PUBLIC AND PRIVATE SERVICES CAN RELY ON TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS CROSS BORDER

MEASURE 3: SETTING SECURITY REQUIREMENTS AND COMMON TECHNICAL STANDARDS FOR THE SECURE EXCHANGE OF DATA LINKED TO IDENTITY

In order to ensure trust, security and a seamless exchange of data necessary for this service, common technical standards will be required. Technical references and / or standards will be needed to: i) access data stored in authentic sources, ii) the provision of verifiable credentials (whether to the person or directly to the online service provider relying on this data) and iii) for hardware and software enabling their secure storage on devices.

The revised regulation would define the functional characteristics of those requirements which will be further specified in implementing acts. To identify the relevant technical references / standards, the Commission would carry out a gap analysis based on available industry standards. In case further

[146] Unless the qualified trust service provider providing the data is also a legal identity provider notified by a Member State under the eIDAS Regulation

[147] These legal identities are provided by Member States' accredited providers notified under eIDAS (see option 1).

[148] This is similar to set-up of the technical infrastructure supporting the once only exchange of data under Article 14 of the Single Digital Gateway Regulation, see https://ec.europa.eu/growth/single-market/single-digital-gateway_en

specifications or standards will be needed, these would be established in cooperation with Member States and stakeholders and with support from the appropriate standardisation organisations (e.g. ETSI).

MEASURE 4: DEFINE THE LEGAL EFFECT OF DIGITAL IDENTITY CREDENTIALS

As is currently the case under eIDAS for other (qualified) trust services, the revised Regulation would establish the principle that a digital identity credential (expressing personal attributes) should not be denied legal effect on the grounds that it is in an electronic format. Qualified attestations of attributes should have the equivalent legal effect of the paper-based credentials they replace. This would provide legal certainty at the European level similarly to what is provided for other qualified trust services. For example, under eIDAS, a qualified electronic signature has the same legal effect of a handwritten signature[149].

MEASURE 5: REGULATED SECTORS SUCH AS ENERGY OR FINANCE AND THE PUBLIC SECTOR WOULD BE REQUIRED TO RELY ON QUALIFIED DIGITAL CREDENTIALS

To further improve the cross-border use of qualified attestations of attributes and credentials, the public sector and regulated sectors such as energy or finance would be required in the Regulation to rely on them to provide the same legal value as paper based attestations of attributes.

MEASURE TO PROVIDE CITIZENS FULL CONTROL OF THEIR PERSONAL DATA AND ASSURE THEIR SECURITY WHEN USING DIGITAL IDENTITY SOLUTIONS

Identity data is personal data, the processing of which is regulated by the General Data Protection Regulation applying as well to new trust services for the secure exchange of data linked to identity and to the providers of legal national eID.

The existing eIDAS framework for trust services provides assurance with respect to the processing of personal data in the case of notified national eIDs. However, to effectively protect personal identity data in a new market where private actors provide authentication services and where identity data will considerably increase in volume, specific requirements are necessary to ensure that market actors implement the rules. For these reasons, it is proposed to strengthen the existing safeguards under eIDAS.

MEASURE 6: LEGAL REQUIREMENTS TO ENSURE THE PROTECTION OF PERSONAL DATA

An effective enforcement of data protection rules, in particular the purpose limitation principle, needs to consider the specificities of the market segment in question and its main dominant actors. A key requirement considered for market actors in this context is ***'Keep Identity Data Separate from other personal transactional / behavioural data'***. The case for this requirement is pertinent to sectors of the digital economy relying largely on the use of personal data raising concerns of unfair competition and the lack of level playing field.

The Digital Markets Act proposal, which lays down harmonised rules ensuring contestable and fair markets in the digital sector, gatekeepers shall refrain from combining personal data sourced from core platform services with personal data from any other service offered by the gatekeeper (such as identity data with other personal data) or from third party services unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679[150]. However, the challenge related to the secondary use of identity data is not limited to large online platforms[151]. Therefore, the following measures are proposed:

---

[149] See eIDAS Article 25 on the legal effects of electronic signatures and article 35 on the legal effects of electronic seals.

[150] Draft DMA regulation, Art 5 (a): "gatekeepers shall refrain from combining personal data sourced from these core platforms with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679"

[151] Yoti Age Scan: in April 2019, Yoti launched a new initiative and potential income stream for the company: Yoti Age Scan technology. This product estimates an individual's age based on their image and is used, for example, within the Yoti app for those who have not uploaded a verified ID document that contains their age; at self-service checkouts to see if an individual is old enough to buy alcohol; to access social media services aimed at teenagers.. Yoti charge businesses to estimate the age of a face. In the case of the use of Yoti outside of the app, a photo of the individual is analysed by Yoti with no other identifying information, and the algorithm decides whether this person is over a certain age threshold. The photo of the individual is deleted and not further stored. Data to train their algorithm is from three sources, including from Yoti users. At the point an individual has a verified ID document on their Yoti account, they are added to the training dataset even though not only the user has no need to use Age Scan within the App. The July 2019 Privacy Policy there was little clarity as to how the users' data was used as part of the Age Scan dataset. There was no accessible way for Yoti users to opt out of use of their data in the training dataset and no accessible way for Yoti App users to request that their data is deleted from the training set without stopping them being able to use the app altogether.

All Trust Service Providers:

The revised eIDAS Regulation will consider imposing the following requirements to *all qualified and non-qualified* providers of trust services for the secure exchange of data linked to identity established in the EU:

- Keep the provision of data linked to identity functionally separate from activity data and other personal transactional or behavioural data or data acquired from third parties not directly related to the provision of the service;
- Offer easy to use opt-in option for every use of identity data for other purposes, accompanied by clear information to the user on how these data will be used and by whom.

These requirements would then be further specified as necessary in technical references and standards against which providers are accredited and audited by national supervisory authorities (the specific supervisory regimes in eIDAS for qualified and non-qualified trust service providers apply).

Qualified Trust Service Providers:

For *qualified* trust service providers for the exchange of data linked to identity, additional measures should apply given the sensitivity of their access to trusted sources from public and private sectors. The following additional principles should apply for qualified providers of such services:

- Keep the provision of data linked to identity structurally separate from activity data and other personal transactional or behavioural data or data acquired from third parties not directly related to the provision of the service[152].

Structural separation would provide users (people and businesses) the necessary reassurance that their data is safe under all circumstances and no additional combination / profiling is possible. It also enhances trust in ensuring that the identity data is not "sold" (beyond where legal obligations/possibilities exist) or traded for commercial purposes. Overall, structural separation would create the necessary trust to ensure uptake and usage of the system by people and businesses. For corporate users, full data security is a commercial and competitive requirement and needs to be ensured particularly for data generated by IoT devices.

Privacy by design would 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 the General Data Protection Regulation. This would mean that providers would need to allow for the selective disclosure of attributes and credentials chosen by the user. It would also mean that services providers relying on the acceptance of digital authentication services would be required to use Application Programming Interfaces (APIs) enabling the selective use of attributes.

All measures to qualified and non-qualified trust service providers would be set out in line with the rights conferred to citizens by the GDPR, which also provide individuals the right to withdraw consent for the processing of their data and will support the implementation of the principle of privacy by design[153].

Creating a market for the secure exchange of data linked to identity would be supported by the following measures put forward under option 1:

- Establish an obligation for Member States to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure ***(measure 1)*** – since the identity data and attributes would be securely linked to the legal eID of the user, notified eIDs are essential to make the data trustworthy and legally enforceable across borders. Streamlining the notification procedure would strengthen the ecosystem of notified eIDs, thus implicitly contributing to this measure.
- *Extend the person identification data set recognised cross border* ***(measure 5)*** – this would ensure identity matching by adding a unique and persistent identifier to the minimum data-set.
- Strengthen Security requirements for mutual recognition ***(measure 6).***

[152] The exchange of data linked to identity as a qualified trust service would be compatible with other neutral brokering functions such as data brokers, personal data space providers as defined in the data governance act.

[153] Article 25 of the GDPR.

MEASURES TO ENSURE EQUAL CONDITIONS FOR THE PROVISION OF QUALIFIED TRUST SERVICES IN THE EU AND THEIR ACCEPTANCE

In relation to ***trust services***, option 2 relies on a similar set of measures as provided by under Option 1.

5.3 POLICY OPTION 3 - HIGH LEVEL AMBITION INTERVENTION: PERSONAL DIGITAL IDENTITY WALLET (EUEID) SUPPORTED BY MEASURES UNDER POLICY OPTIONS 1 & 2

This option aims to ensure that a European Digital Identity personal Wallet App would be made available, on a voluntary basis, to all residents and companies in Europe.

The wallet would empower users to securely share data related to their identity to public and private online service providers through their mobile device and allow them to control their own personal data in a user-centric way. Further to legal requirements, common standards and/or technical references for the Wallet App would be developed in close dialogue with Member States and private sector stakeholders.

The Wallet App would allow the user to integrate a national eID (notified under option 1) and various credentials obtained from private and public providers (issued in accordance with the framework under option 2) and link them to specific identification and authentication services.

Hence, the measures establishing the European digital wallet ecosystem need to rely both on measures put forward under option 1 aiming to strengthen the framework for notified eIDs, indispensable for the trustworthiness of its cross-border use and on measures under Option 2 allowing the establishment of a trust service for attestation of attributes enabling a multitude of use cases, particularly in the private sector.

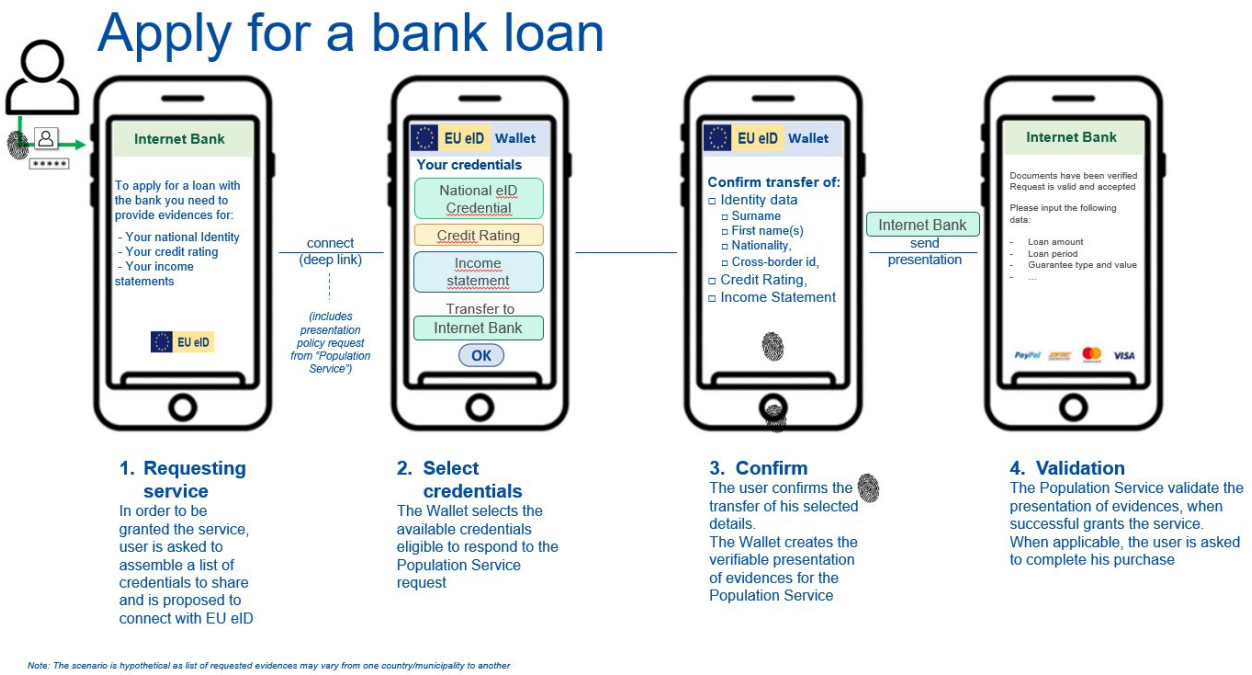
To guarantee a high level of trustworthiness, and therefore to ensure that the user can receive and exchange qualified electronic attestations attributes and credentials related to their identity, the provider of the European Digital Identity Wallet App would need to ensure that the Wallet App can be linked to a national eID or eID credentials.

Two ***sub-options*** are considered for the deployment of the wallet: (1) deployment by private qualified trust service providers under eIDAS and (2) deployment by governments, under their mandate or recognised by them, independently or as an extension to notified eID solutions. Policy option 3 sets-up an ambitious framework that would enhance the exercise by the European citizens of their citizenship rights (Article 20 TFEU) under common rules across the EU.

According to most stakeholders consulted, digital identity wallets are perceived as the most appropriate instrument allowing users to choose when and with whom private services providers can share various attributes, depending on the use case and the security needed for the various transactions. The results of the Open Public Consultation indicate that a large majority of respondents **(63%)** would welcome the creation of a single and universally accepted European Digital Identity scheme, complementary to the national publicly issued electronic identities.

The figure below shows a typical use-case (application for a bank loan) which would allow the user to complete the process fully online with the help of several credentials (national ID credential and credentials testifying credit rating and income) that are carry legal effect as they are linked within the user's personal wallet to the national eID.

Figure 7 - Visual representation of a possible use case for the European digital identity Wallet App



To implement this option, the following measures are considered[154]:

MEASURES TO PROVIDE ACCESS TO TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS THAT CAN BE USED CROSS BORDERS, MEETING USER EXPECTATIONS AND MARKET DEMAND

MEASURE 1 - SUB-OPTION 1: CREATING A NEW QUALIFIED TRUST SERVICE FOR THE PROVISION OF A USER-CONTROLLED SECURE EUROPEAN DIGITAL IDENTITY WALLETAPP

This measure only applies if sub-option 1 (deployment of the wallet by private trust service providers) is retained.

The current set of trust services under eIDAS would be complemented with a ***new qualified trust service*** for the provision of a user-controlled secure European Digital Identity Wallet App. Accompanying provisions in the revised Regulation would establish implementation powers for the Commission to adopt implementing acts detailing the overarching standards needed to ensure interoperability and the functionality of the system.

The Regulation would set the conditions for private providers to develop, distribute, manage and maintain the European Digital Identity Wallet App. The requirements applicable to the Wallet would aim to ensure that it meets ***high security and privacy requirements*** (see below, measure 2).

Specific data protection measures (see Option 2, Measure 6) would apply also to qualified trust service providers from the private sector providing the European Digital Identity Wallet, notably the obligation to keep these qualified trust services structurally separate from other services provided[155].

Some provisions might need to be introduced as regards the costs. Thus, it could be foreseen that qualified trust Wallet service providers should cover the costs of development, distribution and maintenance of the wallet (with available support by European funds under the DIGITAL EUROPE programme). While it would be in principle up to the Wallet provider and other relevant actors to define their business model, it could be foreseen that the wallet is free of charge for the user while costs incurred by Member States providing access to national eID and costs by wallet providers could be covered by the fees obtained by the wallet provider from online service providers relying on the wallet/credentials. Other business models could also be envisaged (see below Chapter 6)[156].

[154] To reach the full potential of the wallet, measures from option 1 and 2 should also be implemented (see chapter 8).

[155] An assessment of impacts is provided under Chapter 5 / policy option 2.

[156] Fees are normally charged by providers of credentials or attributes to online service providers accepting those credentials and attributes.

The general requirements for the conformity assessment/certification and supervision of qualified trust service providers laid down in the eIDAS Regulation would apply, including on liability, technical and organisational measures to manage risks, the security of the services provided, reporting requirements[157], training requirements for staff, the use of trustworthy systems and products, security assessment schemes for relevant components, validation and authentication, etc.

MEASURE 1 - SUB-OPTION 2: EXTENSION OF NOTIFIED EID SCHEMES, OR PROVISION OF A USER-CONTROLLED SECURE EUROPEAN DIGITAL IDENTITY WALLETAPP BY MEMBER STATES (TO BE IMPLEMENTED VIA AMENDMENT OF THE REGULATION)

This measure only applies if sub-option 2 (deployment of the wallet by Member States) is retained.

The eIDAS Regulation would be amended to add the provision of the European Digital Identity Wallet App by Member States. Wallets could be notified either as extensions of their current notified eID schemes or as self-standing solutions. Member States could notify: 1) solutions provided by the government, 2) solutions entrusted by the government to the private sector; 3) solutions provided by the private sector but recognised by the government. In addition, there is a choice to be made on the degree of obligation to Member States to provide the wallet. A voluntary provision would risk the same implementation problems as eIDAS faces today where only 15 out of 27 Member States have notified eID under eIDAS to date.

In bilateral meetings with the Commission, Member States highlighted the need to build a European Digital Identity Framework on the experience and strength of systems developed by Member States and ensure that digital identity in Europe should remain anchored in national registers to provide trust and security.

Some provisions would be introduced as regards the bearing of costs. They could foresee that Member States cover costs of development, distribution and maintenance of the wallet directly (European funds, would be available). The wallet should be free of charge and voluntary for the user while costs incurred by Member States providing access to national eID could be covered by fees applicable to transactions managed by the wallet. Other business models could be possible (see below Chapter 6). Liability would be regulated along art. 11 of the eIDAS Regulation whereby Member States are liable for their eID schemes.

- If The establishment of the wallet ecosystem (irrespective if sub-option 1 or 2 is retained) it would be supported by the following measures put forward under option 1 & 2:
    - Establish an obligation for Member States to offer eIDs and to notify them under the eIDAS, facilitated by a streamlined notification procedure (***measure 1***) – The link between the wallet and the notified eIDs would support the trustworthiness and the security of the wallet, particularly in the context of cross-border transactions.
    - to simplify and improve the notification and peer review procedures (***option 1, measure 2***). As the wallet will be part of the mutual recognition ecosystem, streamlining the notification and the peer-review procedures will facilitate the notification of the national eID schemes relying on a wallet.
    - extend the person identification data set recognised cross border (***option 1, measure 5***). An extended minimum data-set will enhance the capacity of the user to rely on the wallet and engage in as many and diverse online transactions as possible.
    - to create a new qualified trust service for the secure exchange of data linked to identity (***option 2, measure 1***). The attributes issued by the qualified trust services for the purposes of the wallet will offer flexibility to the users to accommodate specific use-cases not covered, for instance, by the minimum data-set.
    - to require Member States to grant access to authentic data to qualified providers of the new trust service for the secure exchange of data linked to identity (***option 2, measure 2***). This measure is needed to enable qualified trust services to issue attributes at a high level of assurance to be asserted via the wallet.

[157] These security and reporting requirements would be harmonized with the new cybersecurity framework in the EU, see https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-uni

- ❖ setting security requirements and common technical standards for the secure exchange of data linked to identity (***option 2, measure 3***). In order to ensure trust, security and a seamless exchange of data necessary in the provision of the attributes to be asserted via the wallet, common technical standards need to be established.
- ❖ to define the legal effect of digital identity credentials (***option 2, measure 4***). This measure is needed to empower users by guaranteeing the legal effect of their credentials asserted via the wallet at European level.
- ❖ regulated sectors such as energy, health and finance would be required to rely on digital credentials provided by qualified trust service providers (***option 2, measure 5***). This measure is needed to facilitate the cross-border use of qualified digital identity attributes and credentials in relation to the transactions where the identity of the users' needs to be ascertained with a high level of certainty.

MEASURES TO ENSURE THAT PUBLIC AND PRIVATE SERVICES CAN RELY ON TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS CROSS BORDER

MEASURE 2: DEFINING COMMON STANDARDS FOR A EUROPEAN DIGITAL IDENTITY WALLET APP (IMPLEMENTED VIA THE AMENDMENT OF THE REGULATION BY SETTING GENERIC FUNCTIONAL REQUIREMENTS, TO BE FURTHER DETAILED IN IMPLEMENTING ACTS)

The European Digital Identity Wallet App will offer a unique personal and mobile platform to exchange credentials and attributes under full control of the user. In order to guarantee interoperability with credential issuers and service providers and meet strict security and privacy levels, performance requirements and related technical standards would be defined. To ensure availability for all citizens, a desktop version of the Wallet App will also be developed.

Four dimensions are linked to the core performance requirements of the European Digital Identity Wallet App and define its business case (see chapter 6):

- ❖ unique personal and mobile platform to exchange credentials and attributes under full control of the user;
- ❖ mobility and accessibility (the mobile character of the European Digital Wallet supports convenience but a desktop solution would be provided to ensure accessibility);
- ❖ coverage of all levels of assurance (scope ranging from simple log-on solutions to identification for eHealth applications etc.)
- ❖ personal data protection and privacy by design [158] (the wallet will enable convenient discretional disclosure of data and guarantee by its design that personal data is private and cannot be seen by service providers, credential providers of wallet providers unless the user consents. This supports the implementation of the GDPR requirements and helps providers manage data security risks)

To define these four dimensions, the following functional requirements would be included in the technical reference framework[159]:

***Security Requirements*:** Security requirements would ensure the App is protected against attackers with high attack potential, duplication and tampering by means of storing cryptographic keys in a secure hardware element inside the device. Not all issuers of certificates might require such high level of protection and it is possible the certificates can be stored on the hard drive of a mobile phone after having been encrypted to ensure confidentiality;

Interfaces: Interfaces towards credential issuers and service providers would be defined as well as requirements for the interface toward the user (look/feel and universal accessibility);

[158] Privacy by design is an approach to systems engineering that seeks to ensure protection for the privacy of individuals by integrating considerations of privacy issues from the very beginning of the development of products, services, business practices, and physical infrastructures.

[159] These requirements would be established similar to existing requirements for electronic means management in Commission Implementing Simplify and Improve ?Regulation 2015/1502 and for signature creation devices in Annex II of eIDAS.

***Functionalities*:** Requirements on basic functionality of the app would be similar to those of eID means or signature creation devices and existing wallets on the market. The purpose of the functionality is to support use cases such as:

- users are able to request identity credentials to the wallet from credential providers as described in policy options 1 and 2,
- notified eID providers or other digital identity providers (such as qualified trust service providers as described in Option **2)** can issue credentials to the wallet,
- the holder of the wallet can see an overview of credentials in the wallet as well as latest transactions,
- the holder of the wallet is able to delete a credential or the wallet,
- the holder of the wallet is able to present identity credentials to service providers for the purposes of authentication and digital signatures etc.
- the wallet can be used for login purposes (i.e. subsequent connections after initial authentication, without the need to provide identity credentials again)
- the holder of the wallet can create self-credentials

Depending on the type of Secure Element used and support from service providers, the Wallet App should support presenting credentials online. Depending on the type of credential, the user may also be able to visually (e.g. displayed on the mobile device screen, including e.g. a QR- or barcode) present the credential from the screen of the mobile phone, including a QR code or similar to retrieve a more complete record for online validation of the correctness of the visually presented data elements.

MEASURE TO PROVIDE CITIZENS FULL CONTROL OF THEIR PERSONAL DATA AND ASSURE THEIR SECURITY WHEN USING DIGITAL IDENTITY SOLUTIONS.

MEASURE 3: SECURITY REQUIREMENTS (GENERAL CERTIFICATION REQUIREMENT UNDER THE REGULATION, TO BE FURTHER DETAILED IN IMPLEMENTING ACTS)

In order to build trust in the cross-border use of European Digital Wallet App, the provider will need to demonstrate how the wallet fulfils the interoperability and security requirements provided by the eIDAS Regulation and relevant implementing acts.

As a security measure, the European Digital Wallet App may be certified in a targeted certification scheme developed under the Cybersecurity Act[160]. Certification would prove compliance with the applicable security and interoperability requirements and performance standards.

- The measures linked to data protection and security of the wallet ecosystem would be supported by the following measures under option 1 & 2:
  - *to strengthen security requirements for mutual recognition (**option 1, measure 6**).* This measure is needed to ensure that components essential for the security of the wallet are certified at the highest level of assurance in line with the state-of-the-art standards for cybersecurity (e.g. against cybersecurity schemes set-up under the Cybersecurity Act).
  - *to establish legal requirements to ensure the protection of personal data (**option 2, measure 6**).* As the wallet should be designed from a user-centric and privacy-enhancing perspective, it is of utmost importance that the qualified and non-qualified trust services issuing the attributes to be asserted via the wallet follow strict requirements liked to the protection of personal data.

MEASURES TO ENSURE EQUAL CONDITIONS FOR THE PROVISION OF QUALIFIED TRUST SERVICES IN THE EU AND THEIR ACCEPTANCE

In relation to ***trust services***, option 3 relies on a similar set of measures as provided by under Options 1 & 2.

[160] REGULATION (EU) 2019/881 introduces a European cybersecurity certification scheme. Art 54(3) provides: "Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act."

5.4 OPTIONS DISCARDED AT AN EARLY STAGE

MEASURE 1 (SUB-OPTION 3): DEVELOPMENT, DISTRIBUTION, MANAGEMENT AND MAINTENANCE BY THE EUROPEAN COMMISSION OR AS MANDATED BY IT

Under this sub-option, the wallet would be developed, distributed and maintained according to common European standards by the European Commission, an existing European agency or by private provider(s) mandated by the European Commission.

The Commission would decide in an implementing act on the governance framework for an own deployment of the wallet or agree terms of reference with Member States to mandate a (consortium of) private companies for a limited duration of time.

Liability would be regulated along Art. 11 of the eIDAS Regulation whereby Member States under certain conditions are liable for their eID schemes whereas the Commission would remain liable for the functioning of the wallet. Commercial liability would apply in case a private operator would be mandated by the Commission to manage the wallet.

This Sub- option has been discarded given that the Commission does not have the necessary permanent technical capacity not only to provide the wallet but also to maintain the underlying services attached to it, and for reasons of liability.

See further details in Annex 5 / Chapter 5, in particular on the development and distribution of the European Digital Identity Wallet.

6 WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

6.1 ECONOMIC IMPACTS

This section presents the main expected economic impacts (costs and benefits) of the different actions available under the baseline and of the measures put forward under each policy option. Under each option, costs and benefits are summarised by stakeholder and further detailed by measure in Annex 5.

The estimates quoted in this chapter are based on mixed-method research including quantitative and qualitative analysis of desk research, survey and interview data combined with economic modelling (i.e. an Input-Output Dynamic Stochastic General Equilibrium Model) which was specifically used to assess macroeconomic impacts on employment and growth. Full details on the methodology used to derive the estimates is provided in the support study for this impact assessment.[161]

An overview of main costs/benefits and their categories can be found in the table at the end of this chapter. The table also highlights the links between the measures and the options.

BASELINE SCENARIO (POLICY OPTION 0)

The table below summarizes the main categories of costs and benefits entailed by the actions considered under the baseline scenario. A detailed description and quantification of the costs and benefits in relation to each action put forward under baseline are presented under Annex 5, chapter 6.

Figure 8 - Baseline scenario - summary of main costs and benefits

Policy option 0 – summary of main costs and benefits		
Measure	**Cost**	**Benefits**
Measure 0.1: Under the DMA, gatekeepers will be required, under certain circumstances, to offer access and interoperability with notified eIDs	Limited compliance costs for gatekeepers	Enhanced security for citizens in using trusted eIDs
		Trusted eID to be re-used by gatekeepers
Measure 0.2: Require Member States to limit identification data transmission to only the data necessary for a particular transaction	Technical adaptations with limited costs for public authorities.	Privacy benefits for citizens in providing only limited data related to attributes

[161] PwC (2021) Study to Support the Impact Assessment of the Digital ID Act

Measure 0.3: Simplify and improve notification and peer-review processes	Costs linked to adaptation to the notification process	Faster mutual recognition benefits for citizens, reduced notification costs due to streamlining of the process
Measure 0.4: Harmonise Supervisory Procedures for Trust Services	Effort in coordination work among national competent authorities, standardisation and legislative process related costs	Reduced need for re-audit from supervisory bodies n/a
		Reduce national divergences in qualifications of TSP

OPTION 1

COSTS

The costs incurred under this option will mainly have to be carried by the ***public authorities*** in the Member States, ***online service providers*** and the ***Commission***. The key costs incurred by the implementation of Option 1 are as follows:

Public authorities:

- Costs directly linked to the notification process for notification of a scheme under eIDAS for the 13 Member States that have not yet done so (estimates between €0.52 and €1.3 million for the remaining Member States)[162];
- In addition, Member States who have not developed fully-fledged eID schemes would incur substantial costs directly dependent on the overall system design, technology chosen and inherent country characteristics (size, population). These costs could range between €40-100 million per Member State (see annex 5 for examples) to develop a scheme from scratch. However, most of these Member States already deploy various types of eGovernment platforms or trusted and secure eID systems allowing their citizens access to public services[163].
- Technical costs for the Member States to upgrade their current operational capacity of the ***interoperability infrastructure*** needed to manage increased levels of traffic once and if all Member States succeed to open their notified eIDs to private sector service providers in the Union (estimated at around €6.1 million across the EU 27)[164]. Opening eIDs to the private sector would require substantial legislative changes at national level, thus triggering additional costs in certain Member States.
- Developing a ***commercial model*** would also incur costs triggered by the coordination and negotiation activities needed between the Member States, followed by costs triggered by legislative amendments at national level. Given the various Members States approaches in terms of monetisation of eID schemes and the difficulty to harmonize the diversity of national liability frameworks (prerogative of the Member States), it is possible that an agreement would be very difficult and lengthy to reach.
- ***Familiarisation costs*** for public authorities in the Member States implied by the legislative changes (with incumbent costs) linked to the extension of the attributes list, requirements for Member States to allow online service providers to rely on notified eIDs, strengthening security requirements for mutual recognition, introducing of e-archiving as a trust service; harmonising remote electronic signing certification.
- ***Compliance costs*** related to certain measures of technical and administrative nature: over the next years costs deriving from the increased workload linked to peer reviews to be completed by the Cooperation Network (€1.2 million overall costs) or costs linked to the standardisation work required to implement the extension of the eIDAS person identification data set recognised cross-border.

National eID Providers or acting on behalf of Member States or recognised by them:

[162] Estimate based on the range of costs per notification provided by Member States through a stakeholder survey. Full details regarding the methodology used are provided in PwC (2021) Study to Support the Impact Assessment of the Digital ID Act

[163] See for example Annex D of Deloitte (2021) Evaluation study of the Regulation no.910/2014 (eIDAS Regulation)

[164] Estimate based on the average technical costs of running the eIDAS node per year (including annual upgrades), provided by the Member States through a stakeholder survey. Full details regarding the methodology used are provided in PwC (2021) Study to Support the Impact Assessment of the Digital ID Act

- eID providers would incur compliance costs stemming from the (voluntary) ***certification*** of eID means under the future EU-wide cybersecurity schemes (estimated at an average €60,000-€120,000 per eID provider) in addition to the costs triggered by any required ex-post adjustment of the eID means and their documentation aligned to certification schemes.
- In addition, the requirement to allow private online service providers to rely on eIDAS-notified eID schemes may require eID providers to adapt their schemes to fit the use-cases in the private sector (e.g. provide the required attributes)

Online Service Providers:

- One-off cost for online service providers for setting up the infrastructure to connect to the eIDAS nodes (the global cost for a relying party could amount to €42,000)[165].

Trust Service Providers:

- Trust Service Providers: TSPs willing to enter the market for qualified e-Archiving services would incur compliance costs similar to those applicable to qualification for other trust services currently covered by eIDAS (an average €545,000 for initial qualification and €255,000 per year on a recurrent basis). Harmonisation of certification for remote electronic signing would also imply adaptation costs.

Commission:

- The Commission would incur costs stemming from the coordination of the legislative amendments, update of the guidance documents, facilitating dialogue with the Member States within the Cooperation Network.

Figure 9 - Policy option 1: overall costs

Policy Option 1 - overall costs		
Stakeholder group	**Overall costs**	**Comment**
Public authorities	Between € 58 million - € 119 million	Among these total costs, between € 50 million and € 110 million will be faced by 13 Member States (as an effect of measures 1.1), while the remaining costs (between €8 and € 9 million) are expected to be one-off costs for all EU Member States.
Online service providers	€42,500 per each provider	These costs are expected for the first year. From the second year onwards only €550 per provider are expected (as an effect of measure 1.8).
Trust Service Providers	€800,000 per each provider	These costs are expected for the first year. From the second year onwards only €255,000 per year per each provider are expected (as an effect of measure 1.6).
Total quantifiable costs	€58+ million	Estimate establishes the minimum total cost of this option, since some cost items cannot be quantified and/or can only be defined by individual stakeholder and not cumulatively.

BENEFITS

Overall, the biggest beneficiary groups of the different measures to reinforce the Regulation are expected to be citizens and end users, online service providers and public authorities, as follows:

- ***Citizens and end users*** would benefit from the mandatory notification of eID schemes by the Member States, as more citizens in the EU would be able to authenticate to online public services provided by other EU Member States. If the commercial model for the use of eIDs by the private sector is established, citizens would also get increased access to private online services on the terms agreed in the model. More transparent and comparable information on eID and trust services would also be made available. Similarly, citizens would benefit from the harmonized conditions for remote signing and from the security brought by the recognition of QWACs by the web-browsers;

[165] LEPS Project. (2018). *D7.2 Report on Cost Benefit Assessment*

- Provided that all Member States open their notified eIDs to the private sector and a commercial model is established, ***online service providers*** connecting to the nodes would benefit from increased certainty and efficiency gains. It would reduce transaction costs and diminish the risks of damages linked to the irregular management of identity data. The ability to rely on an extended eIDAS person identification dataset would also make eIDs more usable across a wider range of use cases thus directly benefiting online service providers in many sectors. Greater reliance by private online service providers on notified eIDs is also expected to increase the transaction volumes within the eIDAS network and generate additional revenues.
- For ***public authorities***, adjusting the notification procedural framework will likely reduce the administrative burden linked to notification of eIDs under eIDAS. The notification of the eID schemes would be smoother as the time needed from the pre-notification of an eID scheme until its publication in the Official Journal of the EU would be reduced making them more quickly available to citizens and businesses for cross border use. Further, the use of EU-wide cybersecurity certification schemes would facilitate ***Member States'*** task to prove compliance of the notified eID schemes with the Regulation.

Figure 10 - Policy option 1: overall benefits

Policy Option 1 - overall benefits		
Stakeholder group	**Overall benefits**	**Comment**
Citizens / end-users	Not possible to quantify	
Public authorities	Between €17 million and €2.5 billion	These benefits are mostly the expected increased revenues in a 5 years period due to measure 1.4
Online service providers	operating expenses reduced by 25% per each provider	Benefit expected on an annual basis
Trust Service Providers	€ 37 million	Benefit expected on an annual basis for every additional 1% of businesses purchasing an eArchiving solution
Total quantifiable benefits	€54+ million	Estimate establishes the minimum total benefit of this option, since some benefit items cannot be quantified and/or can only be defined by individual stakeholder and not cumulatively.

OPTION 2

COSTS

The costs incurred by policy option 2 would mainly fall on public authorities, trust service providers/credentials providers and online service providers.

- For ***public authorities***, costs can be envisaged **1)** to make data stored in authentic sources available to trust service providers for the secure exchange of data linked to identity which may include API integration (cumulatively around €625 million on a one-off basis, EU wide) and €162 million per year on a recurrent basis. **2)**, for additional supervisory duties to accommodate the establishment of the new trust services for the provisioning of attributes, i.e. national level enforcement costs and costs to familiarize with the new regulatory framework. **3)** related to international standard-setting decisions linked to committee work in synergy with standardisation bodies or multi-stakeholder consortium.
- Costs would also be incurred by the ***Commission*** linked to the establishment of the legal framework, in particular adoption of the secondary legislation enabling the free flow of attributes Europe wide.
- ***Trust Service providers/Digital credential providers*** seeking to offer the new trust services, particularly in their qualified form, would face compliance costs: one-off costs for the initial qualified status accreditation, recurrent compliance costs and cost linked to the technical changes to bring the attribute service up to the standards prescribed by the Regulation. Costs would also be incurred to ensure the structural and functional separation of identity data.

- ***Online service providers*** - costs incurred by online service providers are mainly linked to IT integration and to the adjustments needed to implement a system of verified credentials and electronic attestations of attributes. The costs will vary depending on the level of integration, the specific use case and the number of standard components that can be used. The online service providers requesting the use of verified electronic attributes would pay the trust service provider for the issued credentials (comparable business model from the payment cards system).

The costs of the measures under Option 1 (as described under Figure 6) supporting the implementation of Option 2 should be considered also as part of the global costs implied by this option (Measure 1 – mandatory notification, Measure 5 - extend the person identification data set & Measure 6 - strengthen Security requirements for mutual recognition).

Figure 11 - Policy option 2: overall costs

Policy Option 2 - overall costs		
Stakeholder group	**Overall costs**	**Comment**
Public authorities	€ 849 - € 910 million	Among these costs, between € 50 million and € 110 million will be faced by 13 Member States (as an effect of measures 1.1), while the remaining €789 and € 800 million costs are exclusive to Option 2 with around € 170 million are expected to be yearly recurrent costs for all EU Member States.
Online service providers	€ 60,000 - € 70,000	These costs are expected for the first year. From the second year onwards only €550 per provider are expected (as an effect of measure 1.8).
Trust Service Providers	€ 2.3 billion	Among these costs, € 540,000 are expected to be yearly recurrent costs
Conformity Assessment Bodies	€339,000	-
Total quantifiable costs	€3.1+ billion	Estimate establishes the minimum total cost of this option, since some cost items cannot be quantified and/or can only be defined by individual stakeholder and not cumulatively.

BENEFITS

The stakeholders expected to benefit from the creation of a European market for the secure exchange of electronic attestations of attributes are ***online service providers, end users/citizens, trust service providers and public authorities.***

- ***Online service providers*** would benefit from efficiencies such as reduced costs of internal processes involving identity data exchanges, reduced fraud damages and fraud prevention costs or reduced costs of storage of attributes and attestations (e.g. because of substitution of paper attestations by their digital equivalents).
- ***End users and citizens*** would benefit from a strengthened legal basis for the protection of personal data and data security, reduced administrative burden from increased digitalisation of services, increased access to secure and convenient digital identity authentication services and greater recognition of digital identity credentials for public and private services across Europe. Implementation of Option 2 would increase the possibilities to actively manage attributes, credentials and attestations (e.g. gender, age, professional qualifications etc.), better user control of data related to digital identity data and new opportunities for personalised online services in a trusted environment where online privacy and protection of personal data would be safeguarded[166]. Assuming all European citizens engage in around 38 online transactions[167] per year involving both identification and the exchange of data linked to identity, the total number of transactions estimated

[166] European Commission. (2020). Inception impact assessment.

[167] The figure is based on the number of yearly transactions using eID at domestic level in EU Member States from the Deloitte evaluation report.

at EU level would be between 11bn and 17bn[168]. Similarly, the new ecosystem for attributes and credentials will bring improved trust in how these are handled by online service providers, enhancing user-control through more transparent terms and conditions of use and less potential for online platforms to engage in unfair competition by preserving user choice.

- The creation of a new trust service for the electronic attestations of attributes is likely to result in a significant expansion of market opportunities for ***trust service providers*** offering services of data exchanges linked to identity, as well as a level playing field and increased legal certainty in all online transactions. For instance, transport companies (car keys, subscriptions), universities (diplomas), business registries (company info), financial institutions (credit cards), credit rating agencies (credit rating info on natural and legal persons) would directly benefit from the services provided by the qualified trust service providers established under the new framework.
- The new trust service would facilitate the access to public services and encourage cross border transactions, thus reducing the ***administrative burden of the public authorities*** associated with the need to process various verifiable proofs and evidences required to access different public services. Similarly, the option would have a positive effect on the take-up of the existing notified national eIDs since the qualified trust service providers will need to rely on them. In addition, the possibility for the public authorities to rely on attributes and credentials sourced from verified and trusted sources in other Member States would support the application of the once only principle cross border and reduce their administrative burden.

The benefits of the measures under Option 1 (as described under Figure 6) supporting the implementation of Option 2 should be considered also as part of the global benefits implied by this option (Measure 1 – mandatory notification, Measure 5 - extend the person identification data set & Measure 6 - strengthen Security requirements for mutual recognition).

Figure 12 - Policy option 2: overall benefits

Policy Option 2 - overall benefits		
Stakeholder group	**Overall benefits**	**Comment**
Citizens / end-users	€350 to €400 million	Quantified cost savings in addition to benefits of Policy Option 1
Public authorities	Between €17 million and €2.5 billion	These benefits are mostly the expected increased revenues in a 5 years period due to measure 1.4
Online service providers	Between € 3.5 billion and € 6.7 billion	These benefits are yearly recurrent cost savings due to measure 2.1, in 4 different sectors: financial services, eHealth, aviation and eCommerce.
Trust Service Providers	€ 37 million	Benefit expected on an annual basis for every additional 1% of businesses purchasing an eArchiving solution (measure 1.6)
Total quantifiable benefits	€3.9 – 9.6 billion	Estimate establishes the approximate benefit range of this option, since some benefit items cannot be quantified and/or can only be defined by individual stakeholder and not cumulatively.

OPTION 3

COSTS

The main costs of an EU Digital ID scheme (Policy Option 3) are expected to be incurred by ***Wallet App providers*** and ***public authorities***.

Wallet App Providers *(under Sub-Option 1) or* ***Member States*** *(under Sub-Option 2):*

[168] The European population using online services ranges annually between 297.8 million and 451.9 million, we estimate that overall annual transactions passing through the eIDAS network in the EU 27 + UK ranges between 1.117 million and 1.694 million. Full details regarding the methodology used are provided in PwC (2021) Study to Support the Impact Assessment of the Digital ID Act

The key costs for ***Wallet App providers*** are estimated at about €10.5 million for the first-time **development** and rollout of a wallet for the first three years. Procuring an app from the private sector may offer substantial savings. Developing a mobile application for each platform (Google Play Store, Apple App Store, Microsoft Store, Huawei AppGallery, other) would also incur costs. Additionally, investment in ***marketing and customer support*** will be needed to stimulate uptake among service providers and end users[169].

The Wallet App would need to be operationalized which would incur costs linked to the ***onboarding*** to the wallet ecosystem of both credential providers and online service providers. Costs would be incurred from the integration efforts and from the need to conclude agreements with credential- and online service providers. Wallet providers would also need to maintain the security and functionality of the App, ensure readiness to deal with incidents, complaints, offer customer support and help desks for end-users as well as ID providers and service providers. Resources would also be needed to prove ***compliance*** with the regulatory functional requirements (e.g. security certification based on standards for the secure operation of the Wallet App on a secure element (SE), as well as standards for its certification). Ongoing standardisation work is likely to speed up the development of this market.

If the Wallet providers chose to use an embedded SE, negotiations with mobile device manufacturers/all relevant mobile network operators would be required to gain access to the SE or eSIM. In case the European Digital Identity Wallet App is secured by means of a SIM card, it would involve signing agreements with relevant mobile network operators, which will incur administrative costs. Once industry standards for the access to and communication with a secure element in the identity environment are available, it is likely that the associated hardware will be made more accessible by all device manufacturers.

Public Authorities:

Public authorities would incur costs linked to the development of standards (overall costs of €1-2 million). Additional costs would arise from familiarisation with the new standards and any required alignment between the new system and the national legislation. If the first deployment sub-option was chosen, the development of the legal framework would also require resources to cover additional supervision activities for public/private Wallet App providers, with costs estimated at around €1.1 million per year across the EU.

Impact of the Wallet App ecosystem on the investments made by the Member States in their national eID schemes

Once the Wallet App will be operationalized, the new ecosystem will co-exist with the eID schemes deployed by the Member States at national level. The aim of developing the Wallet App is not to replace the current national identity systems or to substitute the entire system of notified schemes under the eIDAS, but to strengthen and reinforce their use. The Wallet App would build on the current eID schemes with the aim to provide the European citizens and companies with functionalities that cannot be offered by the identity systems developed at national level, minimizing stranded costs. More precisely, the current national eID schemes will be the main trust anchors used to onboard the users to the wallet (the same applies for the attributes and credentials issued under Option 2). The anchoring of the Wallet App in the current eID systems will capitalise on Member States investments in their national identity systems.

The existing notified eIDs are not built on common standards, however, for the purposes of accessing online public services across borders, interoperability is ensured using the so-called nodes (see above Section 1). The cost for setting up and maintaining the nodes and the common infrastructure is mostly covered by the Commission though the Connecting Europe Facility (CEF) programme. Since the EU Wallet will be based on a common design and common standards from the outset it will not be necessary to rely on the nodes system. This means that, in the long term, depending on the take-up of the Wallet App, there might be a shift in user preferences and less demand for other identification means to access cross borders services. Consequently, this would trigger gradual cost savings for Member States, the Commission and online services providers since the system of the nodes would be less used when citizens rely instead on the versatility and security of the wallet. In this scenario and given the quick succession of technologies in this area, investments made will be written of by the time existing nodes may fall out of use and it may be decided to discontinue them.

[169] The Wallet currently being developed by Germany is € 5 million.

It will be important to develop a sustainable ***business model*** for the wallet, which will depend on the sub-option chosen for its deployment. It is unlikely that consumers would be ready to directly pay for the app. While the business model would not be fully prescribed by the revised Regulation, the App provider would seek to cover costs by billing online service providers relying on the providers of digital identity services (trust services providers in Option 2).

Under Sup-Option 2, public authorities would carry the costs of the Wallet (see above).

The costs of the measures under Option 1&2 (as described under Figure 6) supporting the implementation of option 3 should be considered also as part of the global costs implied by this option.

Figure 13 - Policy option 3: overall costs

Policy Option 3 - overall costs		
Stakeholder group	**Overall costs**	**Comment**
Public authorities	€ 849 - € 910 million	Among these costs, between € 50 million and € 110 million will be faced by 13 Member States (as an effect of measures 1.1), while the remaining €789 and € 800 million costs are exclusive to Option 2 with around € 170 million are expected to be yearly recurrent costs for all EU Member States.
Online service providers	€ 60,000 - € 70,000	These costs are expected for the first year. From the second year onwards only €550 per provider are expected (as an effect of measure 1.8).
Trust Service Providers	€ 2.3 billion	Among these costs, € 540,000 are expected to be yearly recurrent costs
Conformity Assessment Bodies	€ 678,000	These are the maximum familiarisation costs expected for CABs due to measure 2.1 and 3.1 (sub-option 1).
Wallet app providers	€10.5 million one off for development and maintenance in the first 3 years + additional recurring costs which depend on the business model and cannot be quantified at the present stage Certification costs under the future schemes developed under the Cybersecurity Act of €80.000 – 100.000 per provider	€10.5 million one-off development and maintenance costs have been estimated for the first three years (see Annex 5 / chapter 6 and table 6).
Total quantifiable costs	€3.2+ billion	Estimate establishes the minimum total cost of this option, since some cost items cannot be quantified and/or can only be defined by individual stakeholder and not cumulatively.

BENEFITS

Overall, the biggest expected beneficiaries of the creation of an EU Digital Identity Wallet App are ***end users/citizens, online service providers, Wallet App providers and public and private providers of digital identity services***.

The Wallet App would enable a "sui generis" service for ***citizens and companies***, namely to manage in one place their different digital identities and their related credentials received from various sources (e.g. education, employment, state, professional associations, leisure, etc.) in order to access public and private services anywhere in the EU. This would mark a tangible step towards fostering a genuine European citizenship and towards adding an important building-block to the Digital Single Market.

Besides the facility to access both public and private services, citizens and companies would directly benefit from the convenience and user-friendliness of the wallet authenticating interface and be able to engage in transactions requiring all levels of assurance (e.g. from login on social media to eHealth applications). The link to secure and highly trusted official national eIDs needed in transactions where a high level of certainty on the identity is required, is one of the main competitive advantages of the wallet. The private sector solutions, including those offered by the online platforms, cannot offer this trusted link to official eIDs. In addition, the wallet would deliver this trustworthiness on top of a similarly convenient user experience to the wallets deployed in the private sector (e.g. Apple or Google Wallets).

This "mobile first", user-centric design and the development of common standards are likely to help create a seamless user experience and strongly support the accessibility goals of the Union. As the European Digital Identity Wallet would enable citizens to manage their own different identities and all associated credentials that they receive from various sources from anywhere in the EU, identity management would be considerably simplified. Access to public and private services would be more user-friendly and secure, thus supporting digital inclusion.

A strengthened privacy-by-design approach could yield additional benefits since the wallet would not require intermediaries in the process of asserting the attributes, thus enabling the citizen to communicate directly with the service and credential providers. The increased data security of the wallet would prevent identity theft, thus preventing financial loss to European citizens. Last but not least, the Wallet App would allow users to store attestations of attributes of "things" which would be securely linked to their identity.

The introduction of the EU eID Wallet App is expected to reduce operating costs for ***online service providers***, likely resulting in costs savings related to credentials issuance/verification, better customer experience and reduced costs due to possible frauds. The savings from reduced fraud could be substantial in the many sectors requiring customer identification.

The savings for public authorities from moving towards a standard-based system like the wallet is linked to the reduction in management costs (compared to the current eIDAS interoperability framework), such as costs associated to on-boarding and integration issues. A standard based systems at the EU level will also provide additional market opportunities. Focused exclusively on access to online public services, the eIDAS interoperability system is less scalable and flexible to integrate private online service providers. Standard based systems also reduce the costs of auditing. Online service providers are also more likely to adopt a standard-based ecosystem thus promoting economic growth. Overall, compared to the current eIDAS nodes system, a standards-based system has the following advantages:

- Better system integration and interoperability***;***
- Simplification of complex eIDAS environment***;***
- Innovation friendliness***;***
- Promoting higher economic growth due to increased market potential.

Wallet App providers will have increased market opportunities, providing access to an increased number of users on both sides of the market (both citizens/users and online service providers).

Existing Identity Providers that issue digital identity means to their users (e.g. governments, but also private actors such as financial institutions, Telcos, etc., procuring services to governments if sub-option 2 is chosen) may find developing a European Digital Identity Wallet App (on their own or on behalf of governments) a financially sustainable alternative to existing means, particularly when it offers revenue opportunities at an European scale.

Providers of identity credentials (as described under option 2) would be provided with considerable market opportunities and incentives to issue personalized credentials and to design new services connected to the Wallet App

For the ***providers of secure elements*****,** the Wallet App would open new opportunities related to the likely increase in sales of secure elements (SE) once the wallet ecosystem is operational.

Finally, ***Conformity Assessment Bodies (CABs)*** would have opportunities to generate additional revenue under this option as a result of Wallet app providers seeking conformity assessments.

The benefits of the measures under Option 1&2 (as described under Figure 6) supporting the implementation of option 3 should be considered also as part of the global benefits implied by this option.

Figure 14 - Policy option 3: overall benefits

Policy Option 3 - overall benefits		
Stakeholder group	**Overall benefits**	**Comment**

Citizens / end-users	€350 to €400 million	Quantified cost savings in addition to non-quantifiable benefits of Policy Option 1
Public authorities	Between €17 million and €2.5 billion	These benefits are mostly the expected increased revenues in a 5 years period due to measure 1.4
Online service providers	Between € 3.5 billion and € 6.7 billion	These benefits are yearly recurrent cost savings due to measure 2.1, in 4 different sectors: financial services, eHealth, aviation and eCommerce.
Wallet app providers	Not possible to quantify	
Trust Service Providers	€ 37 million	Benefit expected on an annual basis for every additional 1% of businesses purchasing an eArchiving solution (measure 1.6)
Total quantifiable benefits	€ 3.9 billion – 9.6 billion	Estimate establishes the approximate benefit range of this option, since some benefit items cannot be quantified and/or can only be defined by individual stakeholder and not cumulatively.

SUMMARY OF DIRECT ECONOMIC IMPACTS

The figure below provides an overview of the main costs and benefits of all three options, articulating the individual cost/benefit items and how they relate to each option.

Figure 15 - overview of main costs / benefits and their categories and highlights the link between measures and options

Policy options Summary of main costs and benefits

	Measure	Cost	Benefits	Related policy options
	Measure 1.1: Establish an obligation for Member States to offer eIDs and to notify them under eIDAS	Compliance with eIDAS related obligations - €9.7 million for public authorities (envisaged only for 13 Member States)	Enhanced digital inclusion for citizens / end-users	1, 2, 3
		Increased administrative burden due to mandatory notification - €0.52 - €1.3 million for public authorities (envisaged only for 13 Member States)	Increased personal data protection and online security for citizens / end-users	1, 2, 3
		Increased administrative burden due to additional peer reviews - €1.2 million for public authorities (in the next two years, cumulative for all Member States)	Increased access to public services through secure eIDs for citizens / end-users	1, 2, 3
		Costs to develop a fully-fledged eID scheme of between €40-€100 million (Member States not having implemented deployed them)	Opening the possibility to notify, enable cross-border recognition of national eID schemes	1, 2, 3
	Measure 1.2: Establish a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs	Infrastructural cost to connect to an eIDAS €42,000 per each online service provider	An upgraded interoperability framework that enables more cost-efficient, direct service provider connectivity with the eIDAS network is likely to increase private sector take-up triggering savings for private sector service providers.	1
	Measure 1.3: Establish a harmonised cost-model and liability rules to facilitate private online service providers to rely on notified eIDs	Upgrading eIDAS nodes infrastructure - € 6,1 million for public authorities across the EU (an average € 225,000 per Member State). Costs linked to the coordination and the negotiation of a commercial model between Member States.	Costs savings in operating expenses up to 25% per year for online service provider	1

	Measure 1.4: Extend the person identification data recognised cross border	Committee work needed for standardisation - €300,000 one off cost for public authorities all Member States	Increase revenues from increased online transactions through eIDAS nodes - €17 to €53 million(assumed revenue €0.01 per transaction) to €797 million to €2,5 billion (assumed revenue per transaction) – for public authorities over 5 years in the EU	1,2,3
	Measure 1.5: Strengthen security requirements for mutual recognition	Compliance costs due to certification - €228,000 for public authorities across EU 27	Increased personal data protection and online security for citizens / end-users Savings of €12,000-24,000 per year and per audit for each eID provider as a result of certification	1,2,3
	Measure 1.6: Introducing new Trust Services	Compliance costs linked to the introduction of a new qualified trust service - €545,000 per each trust Service Provider (one-off) and €255,000 per each trust Service Provider (recurrent costs)	Increased revenues due to the introduction of eArchiving - €37 million a year for every additional 1% of businesses purchasing an eArchiving solution - for Trust Service Providers.	1,2,3
			Enhanced offer in the Trust Services market for citizens / end-users	1,2,3
	Measure 1.7: Harmonise the certification process for remote electronic signing	Costs related to compliance with new certification process for Trust Service Providers	Increased competition and security of trust services and acceptance of mobile trust services for citizens / end-users	1, 2, 3
	Measure 1.8: Strengthening the recognition of QWACs	QWACs-related compliance costs approx.; €550 per year, per online service provider	Cost savings from reduced damages related to cybercrimes for citizens / end-users	1, 2, 3
			Increased personal data protection and online security for citizens / end-users	
	Measure 2.1: creating a new qualified trust service for the secure exchange of data linked to identity	Familiarisation with new procedures and standards - €315,000 for public authorities (one-off) Across EU 27 Enforcement and administrative costs due to the introduction of new trust services - €8 million for public authorities per year (recurrent costs) Across EU 27 Cross-border cooperation activities on trust services today €25,000 to €90,000 for public authorities per Member State, could be expected to increase moderately with the addition of new trust service	Cost savings due to reduced operational expenditures in identification procedures ● €0.68 billion to €1.36 billion - for online service providers in the financial services sector per year ● €1.26 billion to €2.51 billion - for online service providers in the eHealth sector per year ● € 30 million to €60 million - for online service providers in the aviation sector per year €0,24 billion to €0.47 billion - for online service providers in the eCommerce sector per year	2,3
		Compliance costs linked to the introduction of a new qualified trust service - €545,000 per each trust Service Provider (one-off) Compliance costs linked to the introduction of a new qualified trust service - €255,000 per each trust Service Provider (recurrent costs)	Cost savings due to reduced expenditures or damages related to cybercrimes ● €0.85 billion to €1.4 billion - for online service providers in the financial services sector per year ● €0.3 billion to €0.6 billion - for online service providers in the eHealth sector per year ● € 3.5 million to €7 million - for online service providers in the aviation sector per year €0.13 billion to €0.26 billion - for online service providers in the eCommerce sector per year	
		Familiarisation with new procedures and standards - €339,000 for Conformity Assessment Bodies	Increased business opportunities for trust service providers	
			Cost savings - €350 to €400 million per year - from reduced administrative burden for citizens / end-users	
	Measure 2.2: require Member States to make available data stored in authentic sources for the secure exchange of data linked to identity	€625 million for public authorities for accessing authentic sources (one-off) €162 million per year for public authorities related to certification (recurrent costs) €18,000 to €27,000 related to integration cost per each online service provider	Cost savings from reduced administrative burden and increased cross-border data exchange for public authorities	2,3

		One-off development of standardised API at EU-level estimated at €30.000		
	Measure 2.3: setting security requirements and common technical standards for the secure exchange of data linked to identity	Committee work needed for setting technical requirements and standards - €1 to €2 million – for public authorities	Enhanced harmonization in the trust service market for Trust Service providers Increased security in the exchange of cross-border data for online service providers-	2,3
	Measure 2.4: define the legal effect of digital identity credentials	Costs for amending the eIDAS regulation in order to modify existing provisions and/or include new ones, for public authorities	Increased recognition of digital identity credentials for accessing public and private services in different Member States for citizens /end-users Reduction in the costs of verification and storage of attributes and attestations for online service providers Increased legal certainty for Trust Service Providers	2,3
	Measure 2.5: regulated sectors such as energy or finance and the public sector would be required to rely on qualified digital credentials	Costs related to IT integration and the upgrade of portals to a new system adapted to the verified credentials and attestations	Legal compliance, legal certainty in relation to the identity of the customers, reduced exposure to damages and identity fraud	2,3
	Measure 2.6: legal requirements to ensure the protection of personal data	One-off cost for functional separation of €30.000 estimated for trust service providers Technical costs related to structural separation of €730,000 (one-off) and €30,000 per year (recurrent) for qualified trust service providers	Increased personal data protection and online security for citizens / end-users	2,3
	Measure 3.1 (sub-option 1): creating a new qualified trust service for the provision of a user-controlled secure European Digital Identity Wallet App	Development and Maintenance costs of €10.5 million for the first 3 years for Wallet App provider Costs of €339,000 linked to familiarisation with Wallet App conformity assessment procedures for Conformity Assessment Bodies Qualification costs of €545,000 (one-off) and €255,000 per year (recurrent) for Trust Wallet app providers Additional operational and marketing costs for Wallet app providers (not possible to quantify) Costs of on-boarding both credential providers and service providers to the ecosystem. (not possible to quantify)	Increased business opportunities for Wallet app providers Increased personal data protection and online security for citizens / end-users Increased access to public and private services for eID providers and citizens / end-users	3
	Measure 3.1 (sub-option 2): provision of a user-controlled secure European Digital Identity WalletApp by Member States	Development and maintenance costs (up to 10.5 MEUR + recurrent maintenance costs)	Increased access to public and private services for eID providers and citizens / end-users Increased personal data protection and online security for citizens / end-users	3
	Measure 3.2 (all sub-options): Defining common standards for a European Digital Identity Wallet app	Cost incurred by the public authorities linked to the standardisation work, building on the existing standards and ongoing standardization activities. In case new standards have to be developed costs incurred are estimated at €1 to €2 million	Deployment of the EU Wallet App based on harmonised standards ensuring consistent user-experience across the EU and transparency on the security requirements and functionalities.	3
	Measure 3.3 (all sub-options): (Introducing) Security requirements	Costs stemming from the certification under the future schemes developed under the Cybersecurity Act - €80.000 – 100.000 per provider	Using certification ensuring an effective way for the Wallet providers to prove compliance with the highest available EU security requirements, user security when transacting online	3

6.2 WIDER ECONOMIC IMPACTS

OPTION 1

Option 1 is unlikely to generate substantial positive effects on GDP and job creation. The ***macroeconomic benefits*** are estimated at €127 million added value generated over 10 years following implementation, of which almost 50% expected already in the first year[170]. Once implemented, this policy option is estimated to generate between 1,5 thousand and 2,8 thousand additional jobs in 10 years across the economy, half of which likely to be created in the first year of implementation.[171]

The measures aiming to enable the use of public eIDs by the private sector will create additional ***market opportunities*** for online service providers who will be able to digitally expand their customer base at EU level. Similarly, the measures aiming to expand the number of private sector use cases that can be supported in the eIDAS network are expected to lead to greater adoption of the notified schemes for private uses, thus increasing the number of ***private sector transactions*****.** The size effect would depend on the extent of private sector adoption and on the choices for use-cases to be technically enabled.

Greater harmonisation brought by ***certification and references to standards*** are expected to help mitigate the national implementation differences currently responsible for some of the frictions in the market for eID and trust services.

OPTION 2

In terms of ***international trade and competitiveness***, a stronger and wider European framework for the provision of trusted electronic identity authentication services underpinned by legal identities provided by Member States can boost global trade and support competitive advantage of the EU-based enterprises. Option 2 could be beneficial, as it would facilitate:

- the creation of a world-class digital identity attribute system that promotes Europe's leadership in this field
- the competitive advantage of European businesses globally, through greater digitalization (and thus, efficiency and effectiveness) of their service offering.

Option 2 may also have a positive effect on ***international cooperation***. An improved and extended framework for the provision of identity and authentication services can increase opportunities for mutual cooperation with other parts of the world, which would directly benefit European businesses. Imitation effects may also ensue in the long term if the new framework delivers on its intended results. EU's regulatory approach for development of legal digital identity frameworks might be followed in other jurisdictions across the globe.

Option 2 is expected to positive impact in terms of economic growth. The general equilibrium model used in the context of this study estimates the amount of added value generated by additional investments and adoption rates triggered by this legislative change. The model considers the impact of additional investments between €100m and €500m and different levels of adoption rates of eID across the economy (ranging between 20% and 67%) for a period between 1 and 10 years. According to the model, once fully implemented, this policy option is going to generate across Europe between €127 million and €1,27 billion added value over a period of 10 years. The majority of the added value is expected to be generated in the first year of implementation (i.e. between €64 million and € 609 million added value in the first year). A summary of the estimated added value generated by the introduction of Option 2 is illustrated in the table below.

Figure 16 - Option 2: Estimated economic impacts in 5 to 10 years according to different levels of adoption[172]

Additional investment	Value added generated (€millions, 2019 prices) - Total by level of adoption, over 5 and 10 years

[170] PwC (2021) Study to Support the Impact Assessment of the Digital ID Act.

[171] Source: PwC (2021) Study to Support the Impact Assessment of the Digital ID Act

[172] Estimates based on the results from an Input-Output Dynamic Stochastic General Equilibrium Model. Full details regarding the methodology used are provided in PwC (2021) Study to Support the Impact Assessment of the Digital ID Act and in Annex 4.

triggered by legislative changes under Option 2 (€millions)	20% adoption				33% adoption				67% adoption			
	1 y	2 y	5 y	10 y	1 y	2 y	5 y	10 y	1 y	2 y	5 y	10 y
€100	€64	€96	€127	€132	€91	€138	€182	€189	€122	€184	€244	€254
€500	€318	€482	€637	€662	€454	€688	€910	€946	€609	€922	€1,220	€1,268

OPTION 3 (ALL SUB-OPTIONS)

Similarly to option 2, this option is expected to have a ***positive impact on innovation*****.** Option 3 takes further measures to promote interoperability via standards, resulting in:

- a stronger effect on innovation, as interoperability can be a driver of innovation in its own right[173].
- a stronger influence on the type of investments demanded in the market. Given the trade-offs to be made between interoperability and technological neutrality, more of the former would mean a stronger signal to the market as to the investments that should be prioritized (i.e. those that are more aligned with the technologies enabling the interoperability frameworks).

Provision of a standardized European Digital Identity Wallet App is expected to result in more significant impacts on ***international trade and competitiveness*****.** Creating a unified, more easily recognisable EU approach internationally would make a positive difference to the EU's ability to raise its global profile in digital identity, foster the competitive advantage of European businesses globally and to cooperate with third countries.

In terms of ***economic growth*** it is expected that the introduction of a standard-based system will reduce uncertainty for market actors to a greater extent than under option 2. The results provided are detailed in a dedicated external study[174], while the figures capture the added-value created by any additional investment and adoption rate that can be attributed to changes in the legislation As a result , the 10-year wider impact of the policy is the same across Options 2 and 3 (for the same level of additional investment and adoption), but likely to be generated more rapidly under Option 3 as market actors would adjust more quickly to the intervention; indeed, a greater proportion of the total impact will arise within the first five years.

Assuming that the policy measures under Option 3 will lead to additional investment in digital identity within a range of between €100 and €500 million, for the first two years after its implementation the impact of Option 3 on economic growth is likely to be higher compared to Option 2: more specifically, in Option 3 the added value is expected to increase by nearly 10% in the first year, 15% in the second year and 2% at the five-year horizon. Via econometric modelling it can be estimated that the wider European economy could generate between around €250 million and €1.27 billion added value over the 10 years following implementation, of which 96% (between around €250 million and €1.24 billion) could be expected in the first 5 years, on the condition that an adoption rate of eID by European enterprises of 67% (i.e. around two thirds) is reached. At lower adoption rates, impacts on value added would be more modest but still positive in net terms[175]. If reducing uncertainty across market actors and eliminating barriers across Member States, the amount of investment generated by Option 3 is likely to be considerably higher than provided in Option 2, generating also a higher impact in terms of additional added value.

Figure 17- Option 3: Estimated economic impacts in 5 to 10 years according to different levels of adoption[176]

Additional investment	Value added generated (€millions, 2019 prices) - Total by level of adoption, over 5 and 10 years

[173] Although the relationship between the two is highly complex and fact-specific. See for example: Gasser, U. Palfrey, P. (2007) When and How ICT Interoperability Drives Innovation. The Berkman Center for Internet & Society, Harvard University

[174] Study to support the impact assessment for the Digital ID Act" by PwC

[175] These figures only capture the value added created by any additional investments that can be attributed to changes in the legislation. As such, it refers to indirect effects only and does not take into account the direct productivity benefits accruing to businesses because of cost efficiencies and an expansion of the market (discussed in the previous section)

[176] Estimates based on the results from an Input-Output Dynamic Stochastic General Equilibrium Model. Full details regarding the methodology used are provided in PwC (2021) Study to Support the Impact Assessment of the Digital ID Act

triggered by legislative changes under Option 2 (€millions)	20% adoption				33% adoption				67% adoption			
	1 y	2 y	5 y	10 y	1 y	2 y	5 y	10 y	1 y	2 y	5 y	10 y
€100	€70	€111	€130	€132	€100	€158	€186	€189	€134	€212	€249	€254
€500	€350	€554	€650	€662	€500	€791	€929	€946	€670	€1,060	€1,244	€1,268

6.3 SOCIAL IMPACTS

OPTION 1

The social impact under this policy option is expected to be positive, however limited on ***employment growth***. Once implemented, this policy Option is estimated to generate between 1,5 thousand and 2,8 thousand additional jobs in 10 years across the economy, half of which likely to be created in ***the first year of implementation*****.** Option 1 has no cost implications for citizens.

OPTION 2

A positive impact on employment is expected from this option via its contribution to the future expansion of online transactions and reduction of barriers in the Internal Market. Taking into account the results from a dedicated external study, the introduction of this policy option is expected to generate between 5,000 and 26,000 additional jobs over the 5 years following implementation, which could be extended to 6,000 and 28000 additional jobs in 10 years, if an adoption rate of eID by European enterprises of 67% (i.e. around two thirds) is reached[177]. This means that indirect effects in terms of job creation will likely be minimal, even at relatively high adoption rates; at the same time, no significant employment loss is likely to occur in net terms despite the strong incentive provided by the option towards digitalization and automation of processes connected to digital identity.

Figure 18 - Option 2: estimated employment impacts in 5 to 10 years according to different levels of adoption

Additional investment triggered by legislative changes (€millions)	Additional jobs generated (thousands) - Total by level of adoption, over 5 and 10 years					
	20% adoption		33% adoption		67% adoption	
	5 years	10 years	5 years	10 years	5 years	10 years
€100	3	3	4	4	5	6
€500	14	15	20	21	26	28

OPTION 3

Option 3 (all sub-options) is expected to generate a positive impact on employment. With regard to the estimates for economic growth effects, more of the expected long-term impact on job creation will be generated within the first five years following implementation if Option 3 is implemented, compared with Option 2 (as market agents are expected to adjust more quickly).

Assuming that Option 3 will lead to additional investment in digital identity within a range of between €100 and €500 million, it is estimated via econometric modelling that the wider European economy could generate between around 5,000 and 27,000 additional jobs over the 5 years following implementation, which could be extended to 6,000 and 28,000 additional jobs in 10 years if an adoption rate of eID by European enterprises

[177] These figures only capture the jobs created by any additional investments that can be attributed to changes in the legislation. As such, they refer to indirect effects only and do not take into account the direct productivity benefits accruing to businesses because of cost efficiencies and an expansion of the market (discussed in the previous section)

of 67% (i.e. around two thirds) is reached[178]. This means that, despite the impact on employment can be considered minimal, no significant employment loss is likely to occur in net terms. An overview of the impacts is illustrated in the table below.

Figure 19 - Option 3: estimated employment impacts in 5 to 10 years according to different levels of adoption[179]

Additional investment triggered by legislative changes (€millions)	Additional jobs generated (thousands) - Total by level of adoption, over 5 and 10 years					
	20% adoption		33% adoption		67% adoption	
	5 years	10 years	5 years	10 years	5 years	10 years
€100	3	3	4	4	5	6
€500	14	15	20	21	27	28

The positive impact on employment could also be explained by the reduced costs for businesses to ***identify relevant and adequate candidates***. In this regard, a pan-European digital ID is likely to facilitate employee authentication, in particular of workers involved in non-traditional jobs such as the gig economy. Thus, reducing the time requested by businesses to find the most appropriate employee for an open position. This is confirmed by the fact that the proportion of job applications undergoing background checks has increased considerably (across 15 percent of the average hiring cycle)[180].

With regard to ***people with disabilities***, the introduction of digital ID is expected to facilitate access to several services, especially provided by the public sector. However, its impact is highly dependent on the level of web-accessibility implemented by the public sector bodies, which currently remains low[181]. In the Open Public Consultation, 36% of respondents report accessibility barriers for persons with disabilities as one of the factors that could limit the use of eID. In this context, the transposition of the European Directive on the accessibility of websites and mobile applications in national legislation is expected to reinforce the benefits associated to Option 3 for this category of persons.

6.4 TECHNOLOGICAL IMPACTS

OPTION 1

European ***certification schemes*** are likely to have a positive impact by incentivising the creation of highly secure eID solutions and by strengthening enforcement of the EU regulatory frameworks in the eID field. Introducing European standards via EU wide certification schemes would also support EU's ***technological autonomy***. Technological sovereignty would also be enhanced through greater harmonisation of the implementation of eIDAS, as regulatory consistency and enhanced seamless delivery of cross-border services constitute supporting factors[182].

OPTION 2

With regard to ***innovation and technological competitiveness***, Option 2 is likely to have a positive impact on innovation, as far as it would:

---

[178] These figures only capture the jobs created by any additional investments that can be attributed to changes in the legislation. As such, they refer to indirect effects only and do not take into account the direct productivity benefits accruing to businesses because of cost efficiencies and an expansion of the market (discussed in the previous section)

[179] Estimates based on the results from an Input-Output Dynamic Stochastic General Equilibrium Model. Full details regarding the methodology used are provided in PwC (2021) Study to Support the Impact Assessment of the Digital ID Act

[180] Why is hiring taking longer? New insights from Glassdoor data, Glassdoor, June 2015

[181] This was first showed by the "Measuring progress of eAccessibility in Europe" (MeAC) study in 2007, and then confirmed by the subsequent studies MeAC 2 (2010) and MeAC3 (2012).

[182] See OECD. 2011. "Communiqué on Principles for Internet Policy-Making." OECD High Level Meeting, The Internet Economy: Generating Innovation and Growth. June 29. p. 3. Such criteria have been used to assess impacts on technological sovereignty in other studies; for example, see Maurer, T et al. (2016). Technological Sovereignty: Missing the Point?. 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace

- Bring to the market solutions that build on the private sector expertise, skills and previous investments. These assets can be leveraged to build more ambitious and cutting-edge eIDAS-compliant solutions in the future, as commercial providers have the resources, know-how and incentives to take on riskier R&D projects.
- Create a more competitive market with independent participation from commercial providers, which would strengthen the incentive to innovate. More competition would encourage providers to gain a competitive edge through value-based differentiation of their products, bringing with it a better ability to achieve a return on R&D investment. Combined with more regulatory certainty, this would have a positive effect on the exploitation of technologies.
- Expand to public procurement of electronic identity and authentication solutions, as the measures proposed provide an opportunity to boost technological development in the field through public procurement processes, particularly with regard to investments that private sector actors may be less well positioned or willing to make (e.g. because returns may be too long-term or not fully appropriable).

OPTION 3

Similarly to option 2, Option 3 (all sub-options) is expected to have a **positive impact on innovation** (see also the section on wider economic impacts).

The measures to promote interoperability under Option 3 would boost the presence and accessibility of secure elements in mobile devices, which in turn could trigger advances in other identity applications and beyond.

In addition, creating an EU eID with wide usability will ensure that more market players have an incentive to invest or encourage investments in cutting-edge digitalisation technologies.

Promoting common European technical standards for a wallet app focusing on a user-determined environment following SSI (self-sovereign identity) principles would benefit innovation in digital identity solutions given the emerging and innovative market shape and the wide scope of the wallet and its user-base. Impacts through standardisation are set out in annex 6, section 7.

Should a standards-based European Digital Identity ecosystem in the medium or long terms make the use of cross-border eIDAS nodes redundant, efficiency savings can be achieved.

6.5 IMPACTS ON SOCIAL INCLUSION AND FUNDAMENTAL RIGHTS

OPTION 1

Option 1 could impact positively EU citizens ***opportunities to live, work and access services*** seamlessly across EU, which are directly dependent on the successful implementation of the measures to allow private sector re-use of notified schemes and of the commercial model supporting cross-border transactions implying private relying parties.

Option 1 has the potential to enhance the ***digital inclusion*** of citizens (particularly disadvantaged groups) since the obligation for Member States to notify at least one eID scheme would provide citizens with universal access to an eID both at national level and in a cross-border context (to be used at least to access public services in other EU country).

A greater availability of eID means will also support digital inclusion of citizens at risk of exclusion, particularly those who transact less online. A wider use of digital identity is likely to generate a positive effect on lower-income categories, as it would allow them to participate in the modern digital economy in many ways such as to assert their rights over digital services they have contracted . Previous research identifies people who lack any form of legally recognised identification as a group that could benefit from access to digital identity. For example, refugees, stateless and forcibly displaced persons who may have fled their home countries without formal identification. Access to digital identities can help these individuals and their families to get access to assistance and basic services (e.g. purchasing a SIM card) These statements are valid also for Option 2&3.

Option 1 has no cost implications for citizens.

OPTIONS 2 & 3

Both options promote better compliance with the provisions of the Charter of Fundamental Rights of the European Union, supporting, in particular:

- ***Freedoms*** – the right to protection of personal data, which would be more effectively upheld to greater availability of highly secure solutions and additional provisions to promote data privacy, security and transparency of processing of identity data.
- ***Equality*** – Increased access to private and public services online can promote the digital inclusion of groups with low digital literacy and/or who may experience significant barriers in accessing services in person, thus supporting the rights of the elderly and the integration of persons with disability, provided that those services comply with accessibility requirements for persons with disabilities. These advantages are however partially offset by the relatively high requirements as regards necessary (safe but costly) equipment on the side of the user (under option 3).
- ***Solidarity*** – Access to services of general economic interest, environmental protection, consumer protection would all be promoted by greater access to services online through more secure and privacy-preserving digital identity authentication solutions.
- ***Citizens' rights*** - greater access to trusted and convenient means available (including EUeID) to access public and private services cross-border support the right to freedom of movement and of residence, making essential transactions easier in particular for European citizens living and working in EU countries other than their own[183].

Higher age groups would also benefit from the introduction of a wallet, as its convenience would facilitate the access to digital services (e.g. social assistance and/or healthcare services). This group would be encouraged to make more extensive use of their identities if convenient and secure solutions were made available. However, benefits are expected to be mitigated by barriers to access to technology, as well as the digital divide experienced by this group.

In addition, wider availability of digital identity is regarded as promoting:

- ***citizen engagement***: more opportunities to engage with services and civic processes online with secure digital identities can encourage participation from citizens who would not otherwise engage with these. For example, in Estonia, 1 in 5 of the over 30% of individuals voting online say they would not vote at a physical polling place.[148]
- More ***inclusive access to public and private services*** linked to public goods such as education and health, to which some social groups currently face some barriers. For instance, citizens with disabilities or living in rural areas have lower access to services that normally require physical presence if not delivered locally. If greater availability of digital identity resulted in more services being accessible online, these groups would disproportionately benefit from the intervention.

In addition, specific to option 3 is expected to generate positive impacts in terms of increased civic participation, privacy-enhancing, secure, and competitive digital basis for personal data management. Compared to the concept of federated identity, which could lead to the accumulation of control into the hands of a few identity providers (IdPs), the European Digital Identity builds an identity framework where the citizen communicates directly with her/his communicating parties (credential providers, service providers). The absence of intermediaries is likely to generate a positive effects.

6.6 ENVIRONMENTAL IMPACTS

ALL POLICY OPTIONS

The overall assessment of the environmental impacts of the three options, vows for greener paper-less and simplified processes enabled by the new identity ecosystems; yet with some caveats. The positive environmental impact is expected to be greater according to the different levels of ambition of each Option, with the first policy option having the most limited environmental effects while Option 3, which is expected to improve to the maximum extent the take up and usability of eID would bring the greenest potential.

[183] The free movement of workers is also a fundamental right guaranteed by the Treaty on the Functioning of the European Union (EU)

To provide an order of magnitude of the impacts in relation to public services we can cite the Italian example. The number of Italian digital identities (SPID) at the end of 2019 was ~5 million. Today, the active users are more than 18 million with a steadily increase of ~1 million users[184] per month. [for instance, the use of SPID went from ~55 million for the entire year 2019 to ~32,4 in the sole month of February 2021], bringing positive impacts on the emissions reduction related to public service delivery.

On the other side, the benefits just presented are partly offset by the increased reliance in both private and public services delivery on online interactions, which requires electricity consumption for the full life cycle of data centres which consume high levels of energy to power the IT equipment contained within them. However, in order to properly assess the environmental impacts it shall be noted that if the energy used by a computational process is renewable, the energy consumed by that process is limited.

6.7 IMPACTS ON SMES

In the context of the digital identity proposal, SMEs are going to be affected in their capacities as eID/trust service providers and as end users. Given the current market situation the large majority of trust service providers in the EU are SMEs, some few are subsidiaries or departments of larger companies[185]. In a wider sense, all SMEs that make regular use of digital services for their business are expected to be impacted. The number of impacted SMEs in EFTA countries that use digital services amounts to about 5 million[186].

A recent survey of SMEs indicates that current uptake of eID (whether or not eIDAS-notified) and trust services is around 17%. In the same survey, around 30% of SMEs reported being in the process of implementing eID/trust services or interested in doing so. Removing commonly reported barriers to SME uptake of eID and trust service solutions, such as complexity and lack of information, is therefore likely to support an increase in uptake up to slightly under half of SMEs (47%), and enable an additional 3 in 10 SMEs to access the benefits estimated. The potential uptake could grow even further with effective awareness raising. About half of the SMEs responding to the survey reported interest in digitalising their business further; yet, 30% indicated that they were not interested in implementing eID/trust service solutions. Narrowing that gap could support an uptake beyond the levels that could be expected by just considering SMEs that currently show interest in adopting eID and trust services, potentially pushing uptake levels beyond 47%[187].

OPTION 1

SMEs as ID/Trust service providers: SMEs would benefit from the measures of Option 1 for a more consistent implementation of eIDAS provisions across Member States to facilitate their business. At the same time, compliance costs associated with policy changes such as security certification affect SMEs disproportionally but also deliver cost savings in the medium / long-term. An estimated saving of €360,000 - €900,000 per year for SME ID/trust service providers from greater harmonisation of audits can be identified.

SMEs as end users: In their capacity as end users, an extension of eID to private service providers (e.g. measures on requirements, extension of data set, cost-liability schemes) could create significant savings for SMEs in online transactions with suppliers, partner businesses and public administrations. Estimates on wider use of eID by citizens in accessing public services online suggest, SMEs would save, on average, 20 hours per year[188]. Assuming that the same saving can be achieved on private service transactions (for a total of 40 hours saved), this average time saving amounts to nearly 200 million hours saved across all SMEs using digital services in EFTA countries, and an associated cumulative saving of €4.1 billion a year (around €800 per SME)[189].

OPTION 2

---

[184] https://avanzamentodigitale.italia.it/it/progetto/spid

[185] Definition of SME ; Overview of trust service providers: https://webgate.ec.europa.eu/tl-browser/#/tl/DE/9

[186] According to Eurostat data, 20% of SMEs are engaged in sales through e-commerce (see Eurostat: Enterprises making e-sales and turnover from e-sales, EU-27, 2009-2018).

[187] https://op.europa.eu/en/publication-detail/-/publication/712f9ce2-5042-11e9-a8ed-01aa75ed71a1/language-en

[188] McKinsey & Company. (2019). Digital identification: A key to inclusive growth

[189] The value of each hour saved is defined as the average hourly labour cost across Member States (source: Eurostat, Labour cost, wages and salaries, direct remuneration (excluding apprentices) by NACE Rev. 2 activity) - LCS surveys 2016 [lc_ncost_r2]

SMEs as ID/Trust service providers: The introduction of a new qualified trust service for the electronic attestations of attributes opens new business opportunities for existing trust service providers / SMEs as they are established in the business and accustomed to the related regulatory compliance requirements.

There will be additional compliance costs for non-qualified providers which will however remain limited as compliance procedures are less demanding[190].

SMEs as end users: SMEs are likely to benefit from the possibility to identify or authenticate their customers which creates efficiency and simplification benefits; SMEs as end-users would benefit from opportunities to exchange enforceable certificates cross-border, thus reducing an important barrier in the market that disproportionately affects smaller providers. SMEs relying on eID/trust services for online service delivery would enjoy better access and a wider range of solutions to choose from. Estimates suggest the costs for identity verification / authentication in some sectors can be reduced by 90%[191]. Assuming that SMEs spend €40 for identity verification[192] and on-boarding of each user, a business on-boarding 500 users a year can save up to €18,000 in costs on an annual basis.

As end-users, SMEs have fewer resources to interact with public administrations and other businesses and would therefore see transaction costs go down more significantly than other types of businesses. As indicated in the previous option, savings from reduced time spent on these transactions would be up to €4.1 billion a year overall, or around €800 per SME[193]. The additional opportunities created by their ability to use a much wider range of attributes and attestations in transactions is likely to expand the potential savings for SMEs beyond this figure.

OPTION 3

SMEs as ID/Trust service providers: Sub-option 3.1 foresees the deployment of the European Digital Identity Wallet as a trust service. This opens new business opportunities for SME ID/trust service providers, although development and certification costs are likely to act as an entry barrier. SMEs would need to identify a strong business case in order to deploy the necessary resources and develop the wallet and conclude agreements with other players in the Wallet ecosystem e.g. credential providers).

SMEs as end users: SMEs may be interested in adopting wallet services for the purposes of business transactions, while larger companies are likely to favour desktop based solutions based on automated processes (e.g. social security companies using dedicated platforms). Integrating the wallet through APIs to consume credentials / attributes and identify or authenticate customers creates costs to SMEs which are however likely to be offset by simplification and efficiency benefits, depending on the specific business case.

Wider impacts summary table

Impact categories	PO 1	PO 2	PO 3
Economic impact	· Expansion of online transactions and reduction of barriers in the Internal Market · €127 million added value generated over 10 years	· Stronger and wider European framework for trusted eID means · €127m - €1268 m added value generated over 10 years	· Boost global trade and support competitive advantage of EU-based enterprises · €130m - €1268 m added value generated over 10 years
Social impact	· Positive impact on employment growth (between 1,5 thousand and 2,8 thousand additional jobs in 10 years across the economy)	· Positive impact on employment via expansion of online transactions and reduction of barriers in the Internal Market	· Positive impact on employment via expansion of online transactions and reduction of barriers in the Internal Market

[190] Requirements for non-qualified trust service providers include the current technical and organisational measures to manage risks to the security of the services provided, reporting requirements, training requirements for staff, the use of trustworthy systems and products, security assessment schemes for relevant components, validation and authentication etc.

[191] McKinsey & Company. (2019). Digital identification: A key to inclusive growth

[192] Customer identification costs for onboarding have been estimated at €30-40 per user. We apply the upper bound estimate to account for the higher costs that SMEs are likely to sustain in these processes due to lower digitalisation.

[193] The value of each hour saved is defined as the average hourly labour cost across Member States (source: Eurostat, Labour cost, wages and salaries, direct remuneration (excluding apprentices) by NACE Rev. 2 activity) - LCS surveys 2016 [lc_ncost_r2]

	· Increased digital inclusion of citizens (disadvantaged groups)	· Between 5 thousand and 26 thousand additional jobs in 5 years which could be extended to a range between 6 thousand and 28 thousand in 10 years if the adoption rate of eID by European enterprises reaches the 67%	· Between 5 thousand and 27 thousand additional jobs in 5 years which could be extended to a range between 6 thousand and 28 thousand in 10 years if the adoption rate of eID by European enterprises reaches the 67% · Increased digital inclusion of citizens and more inclusive access to public and private online services linked to public goods
Technological impact	· Strengthened EU regulatory framework · Increased EU technological autonomy and sovereignty	· More investment in user-friendly, secure solutions building on innovative technologies · Innovation stimulus via public procurement	· More investment in user-friendly, secure solutions building on innovative technologies · Innovation stimulus via public procurement
Fundamental rights	· Increased opportunities to live, work and access services seamlessly across EU	· reduced risk of ID theft and greater access to trusted and convenient means available to access public and private services online · Increased equality through the removal of barriers to access to public and private online services · Increased access to services of general economic interest, environmental protection, and consumer protection through more secure and privacy-preserving digital identity solutions · Strengthen freedom of movement and of residence, by easing essential digital transactions	· reduced risk of ID theft and greater access to trusted and convenient means available to access public and private services online · Increased equality through the removal of barriers to access to public and private online services · Increased access to services of general economic interest, environmental protection, and consumer protection through more secure and privacy-preserving digital identity solutions · Strengthen freedom of movement and of residence, by easing essential digital transactions · Positive impacts in terms of more democratic, private, secure, and competitive digital basis for personal data management
Environmental impact		· Limited but positive environmental impact due to the extended substitution of paper-based procedures with digital procedures.	

7 HOW DO THE OPTIONS COMPARE?

7.1 EFFECTIVENESS

Effectiveness describes the extent to which the proposal is expected to generate effects that are consistent with the policy objectives set.

OBJECTIVE 1: PROVIDE ACCESS TO TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS THAT CAN BE USED CROSS BORDERS, MEETING USER EXPECTATIONS AND MARKET DEMAND

Option 1 is expected to partially achieve this objective. If implemented by Member States in a coordinated manner, the measures would potentially lead to eIDs available to all EU citizens and companies even if mainly for the public sector and with the costs associated to the mutual recognitions system. The

shortcomings linked to the current design of the trust-building mechanisms under eIDAS and the barriers to notification would only partially be alleviated by streamlining the peer-reviews and the notifications processes.

Compared to the baseline, ***Option 2*** is expected to provide a major contribution to this objective, without however fully achieving it. The new trust service for the provision of credentials is expected to provide a significant boost both to the EU citizens' access to trusted digital identity solutions, i.e. as regards exchange of digital attributes, and to therefore considerably their possibilities to engage in online transactions. Compared with option 1, option 2 provides a more effective response to the issues identified with low private sector re-use of eIDAS schemes. As mentioned in the description of Option 2, the contribution to achieving this objective would be dependent on the Member States having notified their eID schemes. Consequently, only citizens of Member States who notified eIDs would benefit from the cross-border legal effect allowed by the qualified digital identity attributes linked to these notified eIDs. Hence, assessment and the successful implementation of Option 2 relies on the strengthening of the notified eIDs system under eIDAS to be completed under option 1.

Option 3 is expected to attain this objective, regardless of the implementation scenarios (sub-options), and would mark a sharp improvement in both the availability of eIDs and of the related digital identity attributes to be used by European citizens cross-border. Due to the similar final functionalities of the wallet and benefits for the user, all sub-options would be equally effective. Compared to Options 1 & 2, all sub-options under Option 3 would provide a more rapid and direct vehicle for universal access to widely usable and trusted eID means by European citizens. It is expected to deliver the greatest level of acceptance by public and private online service providers. The wallet will enable the availability and use of both primary identity data (notified eIDs under option 1) and of a wide spectrum of digital identity related attributes (qualified or non-qualified attributes, as developed under option 2) that can be unlocked only by the user in a wide range of use-cases. The wallet would act as a single sign-on for all the digital identity data of the users. These features will allow maximum flexibility in accessing and managing both qualified and non-qualified attributes and eID related data, which cannot be achieved under options 1 & 2.

It should be noted that the assessment of Option 3 to fulfil this objective is dependent on a series of assumptions and external factors. Firstly, Option 3 has some inherent limitations in terms of possible outreach to citizens and companies which stem from the high level of security to be set for the wallet via standards, in particular if Wallet providers or Member states consider that a hardware element with enhanced security features - i.e. an embedded secure element (eSE) or an embedded SIM card (eSIM) is necessary. However, other solutions not requiring the use of embedded elements can be envisaged. It is also likely that market developments and recent standardisation processes accelerate the full availability of secure devices. The availability of such devices is expected to grow exponentially and even become omnipresent, at some point and by the time of adoption of the proposal, driven by the penetration of mobile demand for secure applications from the private sector. Overall, if pursued, Option 3 has in itself potential to boost the demand for secure elements in mobile devices. A desktop alternative deployment of the wallet would also cover substantially the use related gaps.

Secondly, full achievement of this objective by Option 3 relies on the capacity of Option 2 to deliver a mature and diversified market for credentials, which would subsequently be used via the wallet.

Finally, similarly to option 2, the on-boarding to the wallet is dependent on the existence of national eIDs notified under option 1, although an alternative solution is foreseen for situations where Member States have not yet notified their eIDs.

Comparing the three options against objective 1 in terms of effectiveness shows that it is only option 3 and the issuing of a European Digital Identity Wallet, relying on most measures set out under option 1 and option, 2 that is expected to fully achieve the objective providing access to trusted and secure digital identity solutions than can be used cross-border, meeting user expectations and market demand. Option 1 and 2 cannot, neither alone nor when implemented together, fully meet this objective.

OBJECTIVE 2: ENSURE THAT PUBLIC AND PRIVATE SERVICES CAN RELY ON TRUSTED AND SECURE DIGITAL IDENTITY SOLUTIONS CROSS BORDER

Option 1 is expected to have a limited potential to improve cross-border and cross-sector use of electronic identities and to support a larger ecosystem of use cases. The measure establishing a requirement for Member States to allow private online service providers across the EU to rely on notified eIDs would provide service providers the opportunity to integrate notified eIDs in their business models. There are

however limiting factors to the establishment of such an obligation which might hinder the success of the option, such as the diversity of national legislation regulating the relationship with the private service providers[194]. Agreeing on a commercial model tailored to the needs of the private sector would raise considerable legal and practical difficulties linked to the need to harmonise national liability regimes, to establish complex pricing and billing strategies, operating models and service level agreements. The same reasoning applies to the definition and addition of additional sector-specific attributes to the current eIDAS minimum data-set, thus justifying the low score for this option. When compared to Options 2 & 3 (sub-option 1), Option 1 offers less flexibility, as opposed to the dynamism and innovative potential of the private sector in developing the sector-specific attributes. Option 1 relies on the definition of attributes based on a heavy intergovernmental decision-making mechanism, while option 2 is supported by the reactiveness and the innovation potential of the open market which is empowered to develop tailored made solutions mirroring specific demands. Furthermore, the current interoperability infrastructure via eIDAS nodes designed mainly for the public sector is too complex to support the possible high demand and number of authentication transactions that the private sector could generate.

Compared to the baseline, ***Option 2*** is expected to provide a major contribution to the achievement of this objective. Option 2 would contribute to this objective by unleashing the potential of the electronic attestations of attributes to be seamlessly shared cross-border. This marks an important progress when compared to the baseline since it would empower citizens and companies to make use of the widest possible diversity of credentials in their digital transactions. Option 2 would contribute to the creation of a genuine market for attestations of electronic attributes and for their exchange cross-border. The success of option 2 is dependent on access to the authentic sources and the notified eIDs to be materialised under option 1. As a stand-alone option, without relying on the supporting measures under option 1, the impacts of option 2 would be limited. Neither on its own nor including the measures set out under option 1 would it achieve the objective to the extent possible relying on the measures set out under option 3.

Only ***Option 3*** would fully address this objective. It has the highest potential to empower citizens to exercise their freedom of movement in any of the Member States. In practice, the European Digital Identity Wallet would provide easy and seamless access to the essential services provided by the public and private service providers, thus simplifying citizens' efforts to establish in other EU Member State or to start a business abroad. Relying only on the electronic identification means notified by Member States under Option 1, alone ir in combination with the provision of electronic attestations of attributes not relying on the availability of an European Digital Identity Wallet, will provide for a limited number of use cases. Option 3 displays the largest possibilities to combine attributes in various ways, ranging from low levels of assurance (e.g. login to various platforms based on username/email and password) to high levels of assurance needed for specific transactions (e.g. banking, telecom, eHealth, diplomas or proofs of membership to a professional association, etc.) although its full potential will only be achieved if Options 1 and 2 are implemented.

Option 3 (and Option 2) are more prone to encourage innovation by stimulating the private sector to invest in the development of a wide range solutions linked to real-life use-case, in a much more flexible way than option 1. For instance, the current KYC providers or data brokers acting at national level, once accredited as qualified trust service providers, would easily expand their business to provide their services cross-border as qualified services under Option 2, to be asserted in the context of a European wallet.

OBJECTIVE 3: PROVIDE CITIZENS FULL CONTROL OF THEIR PERSONAL DATA AND ASSURE THEIR SECURITY WHEN USING DIGITAL IDENTITY SOLUTIONS

Option 1 would bring a major contribution to the security of notified eID solutions by opening the use of the voluntary certification schemes to be established at EU level by the Cybersecurity Act based on objective security standards. On the data protection dimension, Option 1 is reliant on the measures to be taken under the baseline. The full alignment of the eIDAS Interoperability Framework to facilitate compliance with the level of data protection introduced by the GDPR would require substantial changes to the current model where the whole eIDAS minimum dataset is automatically shared with the online service providers. Under the baseline, such an evolution would require major adjustments to the current infrastructure to enable new privacy and data protection features such as selective disclosure, pseudonymisation or unlinkability. It is

[194] In some Member States – e.g. the Netherlands - the reliance of private sector on the national eIDs is open only to the bodies with a public mission).

likely that such steps would require additional investments and complex negotiations between the Member States that might not be concluded on a short-medium term perspective.

Option 2 would attain the objective. The measures under this option have the potential to safeguard the data protection level required by GDPR to a larger extent than Option 1. The new trust service would support more robust data protection, privacy and user control. Besides the requirements on providers of trust services for the electronic attentions of attributes, Option 2 goes a step further and establishes strict requirements for qualified trust service providers to query data from trusted, authentic sources. Specific measures in Option 2, such as keeping identity data functionally or structurally separate from other personal data, are strong safeguards for trust between the trust service providers and users. Option 2 would also rely on the opportunities offered by the voluntary certification schemes to be established at EU level and on the certainty brought by the security standards referenced by the Cybersecurity Act, thus achieving the objective.

Option 3 is the only of the three options that would fully achieve this objective. Under both implementation sub-options (wallet developed by qualified trust service providers or by the Member States), the data protection safeguards under option 2 are also fully integrated and applicable under option 3. The added value and the competitive advantage of the wallet when compared to the solutions under option 1 & 2, is that it will offer similar convenience compared to the social login solutions or to the password managers available on the market. In addition, it will provide a much higher level of security (also relying on the voluntary certification schemes to be established under the Cybersecurity Act) and new privacy friendly ways to manage identity data, thus better protecting the user and providing a higher level of user satisfaction. The wallet will provide unique features when compared to options 1 & 2, namely empowering the user to be in full control over which personal data are shared with whom, while the recipient service provider will be able to quickly verify the requested data, strictly limited to the purposes of that respective transaction.

OBJECTIVE 4: ENSURE EQUAL CONDITIONS FOR THE PROVISION OF QUALIFIED TRUST SERVICES IN THE EU AND THEIR ACCEPTANCE

In relation to trust services, as mentioned in the description of the options, they build on the same level of ambition when compared to the baseline and rely on a similar set of measures.

Given the regulatory intervention considered, all options would equally attain the objective by addressing the identified problem and drivers: a new trust service for e-archiving would be established, thus avoiding fragmentation at the European level, the current divergent practices on remote identification and remote signing would be removed, while web-bowsers would ensure support and interoperability with the Qualified Website Authentication Certificates QWACs.

7.2 EFFICIENCY

Efficiency considers the extent to which the options incur compliance and administrative burden for (i) eID/trust service/Wallet App providers, service providers and other and businesses as end users and (ii) compliance and enforcement costs generated to public authorities in relation to potential benefits.

Compliance and administrative burdens generated for eID/trust service/Wallet App providers, service providers and other businesses as end users

Even if ***Option 1*** will improve the current regulatory framework and address inconsistencies, it is likely to produce a modest reduction of administrative costs and burden for eID providers. Certification of eID means is expected to result in a slight increase of the regulated businesses costs. The latter may represent a net cost in the short term, but is expected to convert into a net benefit and, since certification would be voluntary, it is an avoidable cost. Adding up savings on compliance with increased market opportunities and related revenues for providers (which the option has also been assessed as likely to deliver), it is expected that the option will benefit this group in net terms. In parallel, allowing private online service providers to rely on notified eIDs can substantially decrease compliance costs for regulated sectors where national eIDs are not yet available for the private sector to use, and especially with regards to cross-border use. This is difficult to quantify precisely (it could reach up to 25% yearly reduction in costs due to operating expenses per each provider), but likely to exceed the costs for providers to connect to the eIDAS infrastructure in certain services in order to reap these benefits while not in others for which the provision of attributes or credential would better suit the needs of online providers at a lower cost.

Similarly, trust service providers willing to provide a new eArchiving service would also have to incur additional compliance costs, which would be highest for those seeking qualified status. The size of the

potential annual revenues is expected of around €37 million revenues for every additional 1% of businesses purchasing a solution, exceeding or proportionate to the compliance costs estimated, in particular bearing in mind that providers that have already qualified to provide other types of trust services will be able to find economies of scale.

Option 2 (measures 2.1 and 2.6) are likely to generate limited additional compliance costs for providers of identity credentials, comparable to those currently incurred by trust service providers. Additional requirements for transparency are expected to generate minimal costs, due to the significant investments already made in response to the entry into force of GDPR. Harmonisation of the legal framework helps trust service providers to cut compliance costs and also support cross border service provision. In parallel, the creation of a new trust service implies that prospective providers would need to bear similar additional costs as indicated there in order to enter (qualified) provision of the new service in question (as in option 1). Despite an increase in costs is expected, benefits (in terms of potential revenues from providing the service, as in Option 1) clearly outweigh the costs of compliance as the market created for the secure data linked to identity would likely be bigger.

Measure 2.5 will create compliance cost of integrating identity credentials for regulated service providers. The cost overall is high, but since the subjects are relatively large businesses, the cost per organisation is relatively low. Further, these expected costs compare favourably to the potential savings accruing to these businesses as a result of greater secure exchange of data linked to identity in customer interactions, namely the potential efficiencies to be achieved in operational costs linked to identification procedures (on-boarding procedures, KYC procedures etc.) and reduced expenditures or damages related to cybercrimes (data theft, online fraud and procedures for online fraud prevention).

The overall size of this benefit is difficult to quantify as it depends on the actual private sector uptake that will be achieved; based on the impacts estimated, it is clear that these benefits are substantial for individual businesses and would likely make a tangible difference to the size of the benefits generated by the eIDAS Regulation even under conservative assumptions about increased uptake, at least in those sectors of the economy where the demand for digital identity solutions is sustained by regulatory requirements and compelling business needs (e.g. financial services, eHealth). In this scenario, citizens/end users (including businesses) also stand to benefit significantly from more efficient and convenient interactions with online service providers and greater transparency and safeguards on data security and protection, so that overall, Option 2 is likely to deliver a net benefit for the ecosystem.

Option 3 will generate significant costs for the eID providers, and limited ones for the service providers. Besides the interfaces, service providers would probably have to cover the costs for Wallet and credential providers if they impose fees. Compared to the baseline, the immediate cost for implementing the option for Wallet providers overweighs the benefits in the short-term, as the required investment is frontloaded while revenues are largely backloaded. These costs would be balanced with benefits after a period of time from the perspective of Wallet providers, depending on the speed at which the market for digital credentials develops (number of users, number of transactions).

At the same time, trust service providers willing to become providers of identity credentials for the app would also see market opportunities expanded, but taking advantage of these would require some upfront investment to adapt their business models and develop innovative services in order to effectively exploit any market gaps arising from the deployment of the EU Wallet app. By contrast, the benefits to online service providers in terms of their ability to offer secure and convenient eID that can be used widely to their customers will materialise more rapidly and at a lower cost (confined to the costs of accepting the EU eID); these would be similar to the benefits outlined in Option 2 in terms of the internal processes that would be improved via adoption of the EU eID (lower operational costs linked to identification procedures, lower costs from fraud prevention and losses) but on a larger scale if wide end-user adoption is achieved. Additionally, a much wider range of businesses beyond service providers (particularly SMEs) would also benefit from the scheme as end-users along citizens, in that it would reduce the administrative burden of business transactions and dealings with private and public entities, particularly when located across borders.

In sum, the net benefit created by this Option creates a net benefit from the point of view of eID providers and businesses largely relies on achieving broad uptake, which impacts the speed and extent to which Wallet providers will recover the initial investment and the number of businesses that can access the benefits on a single, secure and convenient eID means at the European level.

Compliance and enforcement costs generated for public authorities

In ***Option 1***, national competent authorities would both see new costs generated and savings on existing costs. On the one hand, the measures aiming to shorten the notification and peer-review related procedures expected to create some modest savings in administrative costs. Additional savings in compliance costs will likely stem from strengthened, more harmonised security requirements for mutual recognition. In addition, taking due account of the caveats expressed in the effectiveness section on the feasibility of implementing a harmonised cost model for private sector parties to rely on notified eID schemes, such a model, if agreed, would generate potential for increased revenues, thus improving the ability of the online service providers to recover their initial investments to integrate the notified eID schemes. Their ability to match identity data accurately would also be enhanced.

At the same time, the implementation of this option will trigger certain new necessary costs. Firstly, public authorities would incur limited additional costs for enforcement due to the need to familiarise with the new legislation, align with new standards and guidelines, upgrade the interoperability infrastructure to support greater exchange of attributes and greater public sector re-use and campaigning efforts. Enforcement costs are expected to vary significantly among Member States, based on their current situation: from being largely cost-neutral for countries that have already aligned with new requirements, while limited costs are expected in those countries requiring significant changes to their operating model. The requirement to upgrade eIDAS nodes to meet new expectations such as selective disclosure and changes to the dataset would require an overhaul of the national infrastructure both on the side of node provisioning and service providers. In addition, increased administrative burden from the mandatory notification of eID schemes and the need to undertake additional peer reviews deriving from it (i.e. compared to a scenario where notification remains voluntary) are likely to increase the overall costs of the eIDAS Regulation for public authorities.

Overall, issuing a definitive estimate of net benefits/costs from the point of view of the public authorities raises quantification challenges(benefits could potentially range between €17 million to €2.5 billion in a 5 years period for all EU member states).That said, it was widely recognised in the stakeholder consultation that the true hidden cost of inconsistencies in the legal framework, lack of harmonisation and low private sector uptake for the whole ecosystem is significant and needs to be addressed to unlock the potential of eIDAS notified schemes in the long term, even if that requires net investment into improving these aspects in the short term.

In the case of ***Option 2***, an extension of the scope of the regulation is expected to generate additional costs due to supervision needed at national level which requires resources to be invested by national competent authorities to cover additional supervision duties raised by the new trust services. While this constitutes a new cost, it compares favourably to the intangible benefits created for the whole ecosystem from enabling a wider range of identity data to be securely exchanged across Europe. Under Option 2, the highest costs for Member States will likely be related to the need to make available data stored in authentic sources. The mandatory set-up cost depends on the scope of data and the number of organisations affected. Quite certainly this will exceed the benefits for public bodies themselves; yet, greater, more secure availability of authentic data cross-border will make it possible to generate greater benefits for the system as a whole, and particularly end-users and trust service providers who will be enabled to use and offer secure eID for a much greater range of private sector use cases across Europe.

Option 3, the provisioning of Wallet Apps as trust services under sub-option 1 will also impose additional costs for national level supervision, which requires resources to be invested by national competent authorities, including in relation to the data protection provisions establishing a new type of trust service. Under Sub-option 2, Member States are likely to incur greater additional compliance costs than under the first sub-option. Supervision costs will stay the same, however the additional obligation for all Member States to notify a Wallet would increase the overall cost to public authorities in this scenario. It is expected, however, that the latter cost may be balanced out by revenues from the Wallet especially in the case of larger markets, due to economies of scale.

Option 3 is very ambitious in terms of the benefits it is set to deliver and the overall investment required. Taking this into account, the option is assessed assuming that appropriate steps are taken to minimise the proportion of costs falling on Member States to only the absolutely necessary activities required to support its implementation.

Overall, with the adoption of Option 2 and Option 3, costs are expected to significantly increase for EU Member States (of around €800 million additional costs) but remaining below the increased revenues expected in a 5 years period for national public authorities (around €2.5 billion for the upper bound).

Overall comparison of quantifiable costs and benefits

Overall, taking into account the economic impacts on all the stakeholder groups,, the total quantifiable costs for Option 1 are expected to slightly outweigh the total quantifiable benefits[195] (net costs of around €4 million), while as a result of the adoption of Option 2 and Option 3 the minimum total quantifiable benefits are expected to be higher than the minimum total quantifiable costs (for both options net benefits ranging from €800 million up to €6.5 billion could be expected)[196].

Moving away from direct costs and benefits the table below provides a comparison of the wider impacts between the different Options in terms of Economic Impact, Social Impact, Technological Impact, fundamental rights and environmental impacts.

7.3 PROPORTIONALITY

As regards the proportionality of the intervention, ***Options 1, 2 and 3*** do not go beyond what is necessary to meet the objectives satisfactorily**.** ***Option 1*** builds directly on the legal basis underpinning the current eIDAS Regulation, introducing elements designed to improve the existing legal framework. It provides a clear contribution to the objectives of improving the functioning of the Digital Single Market through a more effective and harmonised legal framework, the focus of intervention being cross-border aspects where the added value of EU action can be clearly demonstrated.

Even if ***Option 2*** entails more substantial costs for compliance and enforcement than ***Option 1***, the costs would likely be outweighed by the significant potential benefits in terms of competition and market growth, as well as benefits for citizens and end users. Such benefits stem directly from an increase in cross-border recognition and acceptance of electronic identity and attribute services, which is a key objective of the revision of eIDAS and is consistent with the principle of proportionality. ***Option 2*** is also designed to tackle the deficiencies of the current framework and provide a regulated environment for private trust services providing attestations of electronic attributes and identity service providers in the EU, creating legal certainty and enforceability that cannot be achieved at the nation level. This includes the risk to data protection, as there needs to be full assurance of separation between identity data and behavioural / activity data on a level commensurate with the level of assurance provided by the identity service provider and the other services it provides. The additional costs generated by this option are designed to support harmonisation and justified on the expectation that they will reduce administrative burden and compliance costs in the long run. The costs linked to the acceptance in regulated sectors of digital identity authentication attributes can also be regarded as necessary and proportionate as far as they support the overall objective and provide the means by which regulated sectors can fulfil legal obligations to legally identify a user.

Option 3**,** building on the relevant measures under ***Option 1 and 2***, is the best aligned option, providing the most appropriate instrument for setting the necessary interoperability structure for the creation of an EU Digital Identity ecosystem building on legal identities issued by Member States and the provision of qualified and non-qualified digital identity attributes. Option 3 also addresses the limitations of the current interoperability infrastructure via eIDAS nodes, designed mainly for the public sector use and too complex to support the possible high demand and the number of the authentication transactions that the private sector could generate. Taking into consideration the set objectives, ***Option 3*** is also considered sufficiently proportionate and the costs likely to be commensurate to the potential benefits. The costs derived from creating and aligning to the new standards (trust service providers and online service providers) cannot be avoided if the objectives of usability and accessibility are to be achieved. Particularly, ***Option 3***, as well as ***Option 2*** intends to harness and build on the investment already made by the Member States in their national identity schemes.

7.4 COHERENCE

[195] As reported in chapter 6, these quantitative eStimates consider only the minimum quantifiable costs and benefits, since some benefit items cannot be quantified and/or can only be defined by individual stakeholder and not cumulatively.

[196] See comment above.

To the extent the current eIDAS framework only partially succeeded in providing wide-spread access to public and private cross-border digital services[197], ***Option 1*** would provide further harmonisation of the market, ***protecting the investments made*** via measures to improve the current legal framework**.**

Options 2 and 3 take a strong stance on data protection and ensure consistency with the GDPR regulation. In fact, the obligation for digital identity providers to differentiate between users' identification data and other data, and for qualified providers of digital identity attribute services, to structurally separate this service from other services, would be a cornerstone of additional privacy-enhancing measures of the eIDAS revision. These initiatives are consistent with the objectives of the Single Digital Market supporting a fairer competition.

By contrast, only ***Option 3*** seems to achieve the objective of developing an EU-wide secure public electronic identification to provide people with control over their online identify and enable access to cross-border digital services[198]. In this respect, Option 3 is the only option that demonstrates full coherence with the political mandate provided by the Council and the President of the European Commission Ursula von der Leyen its State of the Union speech on the 16th of September 2020.

This option is also the most coherent with overarching EU priorities since it provides the widest range of policy interventions to meet those priorities comprehensively and provide the best fit for EU priorities linked to the digital economy as set out in the strategy Shaping Europe's Digital Future.

All three options help to support implementation of GDPR under eIDAS. With the enforcement of the General Data Protection Regulation, the demands and requirements for the handling of sensitive personal information have greatly increased. Article 32 of the GDPR demands that organisations implement appropriate measures to ensure the security of personal information, and the first example of a measure to achieve this is pseudonymisation.

Transversal measures to the three policy options provide elements in addressing consistencies with other key regulations such as the new Cyber Security Act. ***All Options*** fulfil a high level of complementarity with the new Cybersecurity Act and its common cybersecurity certification schemes. The technical specifications and procedures for assurance levels of the Cybersecurity Act LoA "High" (penetration testing) substantial (conformity), basic (self-certification) could be formally linked with the LoA of the eIDAS regulation overhaul. Also, the need for IoT unique identity from eIDAS ensures consistency with the Cybersecurity Act and the need to cover a broader range of actors on top of persons and companies such as machines, objects, suppliers and IoT devices. The strongest alignment with the Cybersecurity Act is provided by the proposal under Option 3, as it is designed to reduce fragmentation in standards and requirements in a similar way as achieved by the Act in the EU security certification landscape. Alignment with the revised Cyber Security Act is also ensured, irrespective of the differences between three options in so far as it has been proposed to regulate the security requirements applicable to trust services providers within the revised Cyber Security Act deleting Article 19 of the eIDAS Regulation.

As is already the case under the current eIDAS framework,[199] the revised eIDAS Regulatory framework will ensure, where feasible, accessibility for persons with disabilities.

Linked to the security aspects of the eIDAS Regulation and the requirements on Trust Service Providers and the security requirements applicable to them, coherence and alignment with the revised Directive on Security of Network and Information Systems have been ensured. According to the revised NIS 2 Directive as proposed, Article 19 of the eIDAS Regulation will be deleted and replaced by the common criteria according to the NIS 2 Directive, also applicable to eIDAS trust service providers.

The draft Digital Market Act has also proposed regulatory measures for gatekeepers that are relevant. Policy ***Option 1*** requires online platforms, including platforms, not to discriminate and be interoperable with legal electronic identities notified by Member States, building on Article 6(f) of the proposed Act. Policy ***Option 2*** will introduce measures to ensure the protection of personal data building on Article 5(a) of the draft Digital Market Act.

---

[197] Results from the evaluation

[198] European Council Conclusions – 9 June 2020

[199] See Article 15 of the eIDAS Regulation

The Single Digital Gateway Regulation (SDGR) has also important touchpoints and is in line with the review of the eIDAS regulation. Its objective is to fully modernise public administrative services and facilitate online access to the information, administrative procedures and assistance services that citizens and businesses need when living or operating in another EU country. All three policy options are consistent and provide foundational elements to support the objectives of making the once only principle operational under the Single Digital Gateway. Policy Option 1 and Policy Option 2 support the SDGR in some respect by providing stronger incentives for adoption by private sector providers, which, if effective, would likely help streamline online transactions considerably (given that the bulk of these occur in the private sector). Yet, Policy ***Option 3*** is the most impactful of the three options in supporting the objectives of the Single Digital Gateway regulation by putting the user in control.

All three options are also coherent with the European Strategy for Data and the proposed Regulation on European Data Governance[200], providing a framework to support data driven applications in cases when the transmission of personal identity data is required allowing users to be in control and fully anonymised. Re-use of attributes and verification based on data available in official registers held by the public sector covered by policy ***Option 2 and 3*****,** is also consistent with the Open Data Directive and its charging framework. Similarly, the three options are coherent and built on the current regime under the EU Anti-money laundering framework[201] to be revised in 2021 and will offer additional flexibility and solutions to allow identification of customers and the transfer of information, which are necessary to comply with the customer due diligence requirements. This will be supported by the measures ranging from the extension of the minimum data-set to the provision of framework for the exchange of specific credentials and attributes defined by the future AML framework. All options, as far at the delivery of electronic identity and attributes rely on the use of mobile devices, will be coherent with the radio equipment directive and the measures adopted under this directive in order to ensure the protection of privacy, personal data and against fraud.

The revised eIDAS Regulation will provide a framework for the provision of electronic identity and electronic identity services in the EU, on which specific sectors can rely to fulfil sector specific legal requirements, for example related to digital travel documents, digital drivers licences etc. Similarly, the future proposal is aligned with the objectives of the Regulation 2019/1157 which strengthens the security of ID cards and residence documents. Under this Regulation, Member States are obliged to implement new identity cards with the updated security features by August 2021. Once developed, Member States could upgrade the new identity cards so that they can be notified as eID schemes as defined under the IDAS Regulation[202].

The future proposal will also contribute to the transformation of the customs domain into a paperless electronic environment in the context of the initiative for developing an EU Single Window environment for customs[203]. It should be also noted that the future proposal will contribute to the European mobility policies by facilitating the legal reporting requirements of the maritime operators set in the context of the European Maritime Single Window environment which will start applying form 15 August 2025[204]. The same goes for the articulation with Regulation on Electronic Freight Transport Information obliging Member States authorities to accept electronic freight information. The European Digital Identity Wallet App will also be able to handle the credentials related to drivers, vehicles and operations required by the EU legal framework in the field of road transport (e.g. digital driving licences / Directive 2006/126/EC). Specifications will be further developed in the context of this framework. The future initiative could also contribute to the shaping of the future initiatives in the field of social coordination services, such as the development of a European Social Security Passport which could build on the trust anchors offered by the notified identities under eIDAS.

---

[200] See, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

[201] 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

[202] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement

[203] On 28 October 2020, the European Commission proposed a new initiative that will make it easier for different authorities involved in goods clearance to exchange electronic information submitted by traders.

[204] European Maritime Single Window environment (EMSWe): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A4407248

Figure number 20 summarises the comparison of the three policy options that have been analysed for the purpose of this impact assessment. Given the diversity of impacts analysed, the symbols are used to grade qualitatively the values reflecting the performance of each option. The grading is based on the balanced assessment of the evidence collected for each assessment criteria (Efficiency, effectiveness, coherence, proportionality) which is itself based on the overall Cost Benefit Analysis. An overview of the grading is provided in figure 21. The wider impacts, in view of underpinning figure 20 and 21, have been summarized in figure 22.

Figure 20 - Comparison of the options overview

OPTION	EFFECTIVENESS	EFFICIENCY		COHERENCE	PROPORTIONALITY
		Cost/ benefit for businesses	Cost/ benefit for public sector		
OPTION 1	●	●●	●●	●●	●●●
OPTION 2	●●	●●●	●●	●●●	●●●
OPTION 3	●●●	●●●	●●	●●●	●●●

Figure 21 - Comparison of the options, scoring (legend)

Effectiveness	***Efficiency:***	***Coherence scoring:***	***Proportionality scoring:***
●*Minor contribution towards objectives*	● *Considerable additional costs non-proportionate to the benefits and difficult implementation*	● *Lacking coherence*	● *Lacking proportionality*
●● *Major contribution but without fully achieving objective;*	●● *Neutral or Increase in costs proportionate to the additional benefits;*	●● *Largely (but not fully) coherent with the evolution of wider policy objectives*	●● *Largely (but not fully) proportionate to the policy problems to be addressed*
●●● *Fully achieving objectives.*	●●● *Increase in costs largely outweighed by the benefits*	●●● *Fully coherent*	●●● *Fully proportionate.*

Figure 22 – Wider impacts summary table

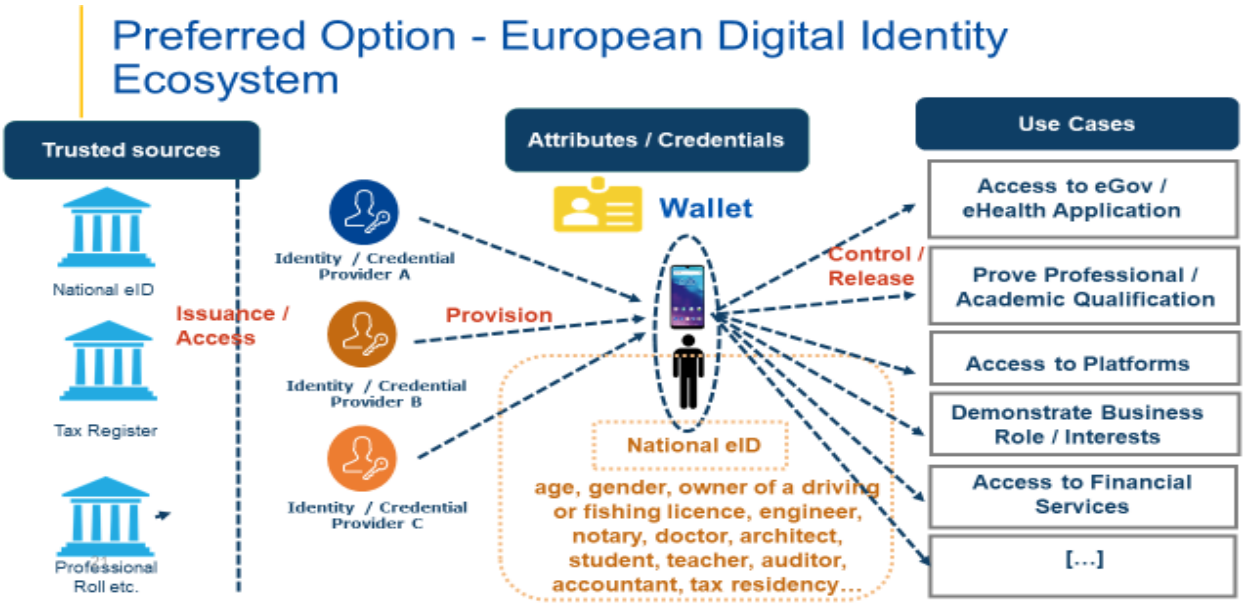
Impact categories	PO 1	PO 2	PO 3
Economic impact	· Expansion of online transactions and reduction of barriers in the Internal Market · €127 million added value generated over 10 years	· Stronger and wider European framework for trusted eID means · €127m - €1268 m added value generated over 10 years	· Boost global trade and support competitive advantage of EU-based enterprises · €130m - €1268 m added value generated over 10 years
Social impact	· Positive impact on employment growth (between 1,5 thousand and 2,8 thousand additional jobs in 10 years across the economy) · Increased digital inclusion of citizens (disadvantaged groups)	· Positive impact on employment via expansion of online transactions and reduction of barriers in the Internal Market · Between 5 thousand and 26 thousand additional jobs in 5 years which could be extended to a range between 6 thousand and 28 thousand in 10 years if	· Positive impact on employment via expansion of online transactions and reduction of barriers in the Internal Market · Between 5 thousand and 27 thousand additional jobs in 5 years which could be extended to a range between 6 thousand and 28 thousand in 10 years if

		the adoption rate of eID by European enterprises reaches the 67%	the adoption rate of eID by European enterprises reaches the 67% · Increased digital inclusion of citizens and more inclusive access to public and private online services linked to public goods
Technological impact	· Strengthened EU regulatory framework · Increased EU technological autonomy and sovereignty	· More investment in user-friendly, secure solutions building on innovative technologies · Innovation stimulus via public procurement	· More investment in user-friendly, secure solutions building on innovative technologies · Innovation stimulus via public procurement
Fundamental rights	· Increased opportunities to live, work and access services seamlessly across EU	· reduced risk of ID theft and greater access to trusted and convenient means available to access public and private services online · Increased equality through the removal of barriers to access to public and private online services · Increased access to services of general economic interest, environmental protection, and consumer protection through more secure and privacy-preserving digital identity solutions · Strengthen freedom of movement and of residence, by easing essential digital transactions	· reduced risk of ID theft and greater access to trusted and convenient means available to access public and private services online · Increased equality through the removal of barriers to access to public and private online services · Increased access to services of general economic interest, environmental protection, and consumer protection through more secure and privacy-preserving digital identity solutions · Strengthen freedom of movement and of residence, by easing essential digital transactions · Positive impacts in terms of more democratic, private, secure, and competitive digital basis for personal data management
Environmental impact		· Limited but positive environmental impact due to the extended substitution of paper-based procedures with digital procedures.	

8 PREFERRED OPTION

This figure illustrates the functioning of the preferred option which puts the user in control of the provision of digital identity attributes based on his national eID. The attestations of attributes by attribute/credential providers are based on official assertions relying on trusted sources in Member States. Using the wallet, the user can identity and authenticate and provide attested attributes to service providers for a wide range of use cases.

Figure 23 - European Digital Identity Ecosystem



In the light of the assessment in Chapter 7, ***Option 3 stands out as the preferred option***, which also has the highest ambition level but is the only option to fully deliver on the objectives set. It should be stressed that Option 3 can only reach its full potential if it builds on other measures put forward under Options 1 and 2.

Option 3 would establish a comprehensive framework providing users with a personal digital wallet to access public and private online services cross-border. In addition, users would be able to carry-out transactions online by storing and managing identity data and sharing electronic attestations of attributes securely in a wide range of use-cases.

Under the preferred option, the following building blocks of measures would reach the objectives set:

Establish a European Digital Identity personal Wallet App ecosystem by:

- Entrusting Member States or qualified trust service providers to deploy it (***Measure 1/PO3 Sub-Options 1 or 2***);
- Setting common standards for the European Digital Identity Wallet with the aim to ensure interoperability with credential issuers (QTSPs under Option 2) and service providers. In addition, reference standards would be required to ensure compliance with the security and functional requirements to be set in the revised Regulation (***Measures 2&3/PO3***).

Enable the free flow and exchange of digital identity data across borders and a strong, trusted link between them and the Wallet App by:

- Extending the scope of the Regulation with a new Qualified Trust Service for the secure exchange of data linked to identity ***(Measure 1/PO2***)
- Requiring Member States to make available data stored in authentic sources, under the full control of the user, for the secure exchange of data linked to identity (***Measure 2/PO2***). This is a pre-requisite for the provision of attributes and credentials by qualified trust service providers.
- Setting security requirements and common technical standards for the secure exchange of data linked to identity (***Measure 3/PO2***)
- Defining the legal effect of digital identity ensuring that digital identity credentials are recognized across borders and are not denied legal effect (***Measure 4/PO2***)
- Requiring regulated sectors to rely on qualified digital credentials in order to improve the cross-border use of qualified certificates (***Measure 5/PO2***)
- Strengthening security requirements for mutual recognition (***Measure 5/PO1***) and ensure that components essential for the security of the wallet are certified in line with the state-of-the-art cybersecurity standards

- Extending the person identification data set recognised cross border ***(option 1, measure 5***) to multiply the opportunities of the users to rely on the wallet (***Measure 5/PO1***)

Ensure cross-border trustworthiness of the Wallet App by linking it to the eIDs notified by the Member States:

- Establish an obligation for Member States to offer eIDs and to notify them under eIDAS, facilitated by a streamlined notification procedure (***measure 1/PO1***)

Ensure data protection and full user control over identity data by:

- Establishing legal requirements to ensure the protection of personal data (***Measure 6/PO2***) - the rules applicable to the issuers of qualified credentials would guarantee the user-centricity of the wallet and the protection of personal data.
- Strengthening security requirements for mutual recognition (***Measure 5/PO1***) would ensure that the Wallet App is equipped with the highest level of security to cover online use-cases at all levels of assurance.

Further to the analysis under Chapter 7, measures 2 & 3 of Option 1 are not retained under the preferred option. If implemented, there would be an unnecessary duplication with the resources needed to establish a standards-based interoperability framework to support the wallet and the cross-border exchange of credentials.

In relation to ***trust services***, the measures retained under the preferred option have a similar level of ambition under all options, implying a robust regulatory intervention. They aim to establish a new trust service for eArchiving, to harmonise the certification processes for remote electronic signing and to strengthen the recognition of Qualified Website Authentication Certificates (QWACS).

The preferred option is in line with the ***subsidiarity principle***, as in this area the EU Digital Single Market cannot be accomplished by Member States at national level. In particular, Option 3 would lead to a more comprehensive, effective and efficient framework in all areas of intervention of this initiative. It will:

- build on the joint efforts of the public and private sectors to provide EU citizens and businesses with an ecosystem of secure and trustworthy digital identity systems, ensuring harmonisation and universal availability of eID means in the EU. This ecosystem would rest on three pillars: the eIDAS notified national eID schemes, a qualified trust service for the secure exchange of data linked to identity and an EUeID wallet that together ensure universal availability, wide usability of eID means in the EU and user control of personal data.
- provide a common reference framework for trust and security and minimum obligations on service providers to support universal acceptance of eIDs in the EU;
- strengthen user control and privacy, allowing citizens to control the provision and use of identity data based on verifiable credentials issued by Member States.

The preferred option does not go beyond what is necessary to address the identified problems and is ***proportionate*** to achieving its objectives:

- the preferred option will build on the existing notified eID schemes and the existing role of Member States as supervisory authorities to ensure a high level of trust in line with a commonly agreed framework.
- The preferred option will neither restrict the role of Member States as issuers of verified identifiers nor propose measures affecting the level of assurance for access to online public services in the EU. The approaches to the use and provision of verified identity credentials, attestations and attributes seek to strike a balance between EU regulation and Member States' public policy interests.

The preferred option is considered future proof in so far as it is content and technology agnostic, providing citizens a portable digital identity solution supporting current trends towards more user centric digital identities available on secure and mobile platforms allowing users to prove who they say they are and verify claims in a multitude of cross border use cases. It accommodates the most recent market developments and embeds the most flexible approach available today to integrate trusted and secure eID provided by Member States and identity attributes provided by a potentially unlimited number of providers. In addition, the option is open to future changes in the technological and legal environment as measures are technologically neutral

and leave room for joint implementation by means of a common set of technical references and standards agreed with Member States. By building on available industry standards, implementation time would be reduced and innovation friendliness and adaptation to changing needs assured. Review mechanisms will further mitigate the risk that technical references and standards fall behind technological advance.

REFIT - SIMPLIFICATION AND IMPROVED EFFICIENCY

Figure 24 - REFIT Cost Savings – Preferred Option (*)

REFIT Cost Savings – Preferred Options		
Description	*Amount*	*Comments*
Savings in administrative costs related to shortening peer-review and notification processes for eID	Overall, of €63.000 in the first year and €220.000 per year afterwards	***Recipient: Public authorities*** *with regards to the baseline which provides to simplify and improve the notification and peer review procedures.*
	Not quantified	***Recipient: Citizens / end-users*** *with regards to the baseline which provides to simplify and improve the notification and peer review procedures.*
Reduced operational costs linked to identification procedures (onboarding procedures, KYC procedures etc.)	Sectoral yearly savings: ● Financial services (overall): €0.68 billion - €1.36 billion ● eHealth: €1.26 billion – €2.51 billion ● Aviation: € 30 million - €60 million ● eCommerce: €0,24 billion - €0.47 billion	***Recipient: Online service providers*** *with regards to option 1 measure 4, which provides to extend the person identification data set recognised cross border, option 2 measure 1 which provides to create a new qualified trust service for the secure exchange of data linked to identity and option 2 measure 5 which requires regulated sectors such as energy or finance and the public sector to rely on qualified digital credentials*
Reduced expenditures or damages related to cybercrimes (data theft, online fraud and procedures for online fraud prevention)	Sectoral yearly savings: ● Financial services (overall): €0.85 billion - €1.4 billion ● eHealth: €0.3 billion – € 0.6 billion ● Aviation: €3.5 million - €7 million ● eCommerce: €0,13 billion - €0.26 billion	***Recipient: Online service providers*** *with regards to option 1 measure 4, which provides to extend the person identification data set recognised cross border, and option 2 measure 1 which provides to create a new qualified trust service for the secure exchange of data linked to identity*
	Not quantified	***Recipient: Citizens / end-users*** *with regards to option 1 measure 8 which requires to strengthen the recognition of QWACs (qualified website authentication certificates)*
Reduced compliance costs (related to security certifications, GDPR requirements)	Not quantified	***Recipient: Public authorities*** *with regards to Option 1 measure 5 which requires to strengthen security requirements for mutual recognition*
Savings in compliance costs related to conformity assessments	€12,000-€24,000 per each audit procedure	***Recipient: eID providers*** *with regards to option 1 measure 5 which requires to strengthen security requirements for mutual recognition*
Savings from reduced administrative burden	Overall, between €350 and €400 million per year	***Recipient: citizens / end-users*** *with regards to option 1 measure 5 which provides to extend the person identification data set recognised cross border, and option 2 measure 1 which provides to*

		create a new qualified trust service for the secure exchange of data linked to identity
	Not quantified	***Recipient: public authorities** with regards to option 2 measure 2 requiring Member States to make available data stored in authentic sources for the secure exchange of data linked to identity*

9 HOW WILL THE ACTUAL IMPACTS BE MONITORED AND EVALUATED?

MONITORING ARRANGEMENTS AND INDICATORS

According to the Better Regulation Guidelines Toolbox Tool #41 the monitoring framework should cover the following aspects of the Regulation:

Implementation: Covers changes to the Regulation and adoption of measures that are necessary to enable the implementation of the selected policy measures.

Application: Focuses on the actual changes observed as a result of the realisation of the policy and is closely linked with the specific and operational objectives. Together with the indicators for implementation, these can be used to monitor enforcement and compliance with respect to each policy measure

Contextual information, if applicable: developments not intentionally related to the Regulation, although they are likely to influence it, such as economic growth, use of new technologies or new behavioural patterns.

The table below presents the indicators and data sources proposed.

Figure 5 - Monitoring Framework: indicators and sources

Monitoring and evaluation aspect and relevant objectives	Indicator	Responsibility for collection	Source(s)
Implementation of adopted changes			
Extent to which necessary changes have been implemented in line with the adopted measure	Extent to which the changes have been completed by a set date	European Commission	Ongoing M&E
Implement necessary changes to relevant national systems	Number of Member States that have completed changes to the relevant system by a set date	European Commission and National Competent Authorities (NCA)	Ongoing M&E
Implement necessary changes to compliance obligations by the regulated entities	Number of regulated entities that have completed changes from new compliance obligations by a set date	European Commission and National Competent Authorities (NCA)	Ongoing M&E
Application			
Provide access to eID means for all EU citizens	Number of European citizens and businesses issued with notified eID-s and number of issued identity credentials.	European Commission and National Competent Authorities (NCA)	Annual survey/M&E data collected by NCAs

Provide access to eID means for all EU citizens	Number of European citizens and businesses actively using notified eID-s and identity credentials	European Commission and National Competent Authorities (NCA)	Annual survey/M&E data collected by NCAs
Increase cross-border recognition and acceptance of eID schemes, with an ambition to reach universal acceptance	Number of online service providers accepting notified eID-s and identity credentials (including on a voluntary basis)	European Commission	Annual survey
Increase cross-border recognition and acceptance of eID schemes, with an ambition to reach universal acceptance	Number of online transactions by notified eID-s and identity credentials (total and cross-border)	European Commission	Annual survey
Stimulate adoption by the private sector and the development of new digital identity services	Number of new privately issued digital identity (eID attribute) services meeting standards for integration into EU Digital identity	European Commission and National Competent Authorities (NCA)	Annual survey
Contextual information			
Stimulate adoption by the private sector and the development of new digital identity services	Size of the market for digital identity	European Commission	Annual survey
Stimulate adoption by the private sector and the development of new digital identity services	Public procurement expenditure linked to digital identity	European Commission and National Competent Authorities	Annual survey
Increase cross-border recognition and acceptance of eID schemes, with an ambition to reach universal acceptance	Share of businesses providing their services online	European Commission	Eurostat
Increase cross-border recognition and acceptance of eID schemes, with an ambition to reach universal acceptance	Share of online transactions requiring strong customer identification (total)	European Commission	Eurostat/ annual survey

Provide access to eID means for all EU citizens	Share of EU citizens using online private and public services (total and cross-border)	European Commission	Eurostat

~ * ~