European Commission

INCEPTION IMPACT ASSESSMENT	
Inception Impact Assessments aim to inform citizens and stakeholders about the Commission's plans in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Citizens and stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to make available any relevant information that they may have, including on possible impacts of the different options.	
TITLE OF THE INITIATIVE	Revision of the eIDAS Regulation – European Digital Identity (EUid)
LEAD DG – RESPONSIBLE UNIT – AP NUMBER	DG CNECT H4
LIKELY TYPE OF INITIATIVE	Regulation
INDICATIVE PLANNING	Q4 2020
ADDITIONAL INFORMATION	*Insert link to "Commission decides" or to the specific website for the initiative*
This Inception Impact Assessment is provided for information purposes only and can be subject to change. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content and structure.	

A. Context, Problem definition and Subsidiarity Check

Context

In its Strategy on Shaping Europe's Digital Future, the Commission has committed to revise the eIDAS Regulation to improve its effectiveness, extend its application to the private sector and promote trusted digital identities for all Europeans.

The eIDAS Regulation, adopted in 2014, seeks to enhance trust in electronic transactions in the single market by providing:

- a common interoperability and mutual recognition framework that allows individuals and businesses to use their own national **electronic identification** schemes (**eIDs**) to authenticate when accessing **public services** in other EU Member States. The mandatory mutual recognition of notified electronic identities (eIDs) applies since 2018[1].

- a regulatory framework for the development of a European internal market for **electronic trust services** (electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication) recognised across borders with the same legal status as traditional paper based processes. This regulatory framework applies since 2016.

With eIDAS, the EU has laid the foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations to safely access services and carry out transactions online and across border. eIDAS solutions reduce red-tape for citizens and create savings for business. Roll-out of eIDAS means higher security and increased convenience for any cross-border online activity that requires trusted identification such as submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another Member State, authenticating for internet payments or bidding to on line call for tender.

As an important element and enabler of cross-border Digital Public Services, the eIDAS Regulation

[1] Adopted on 23 July 2014, the Regulation entered into force on 17 September 2014. However, application of certain provisions of the Regulation was deferred, until 2016 for the provisions on trust services and until 2018 for the mutual recognition of notified eIDs.

contributes to achieving the single market. Recognition of eIDs under eIDAS is key for the cross border application of the "once only" principle, one of the main elements of the Single Digital Gateway.

Electronic identification can be seen as the digital equivalent to presenting an ID card[2] or passport in the physical world. In that sense, electronic identification is a key component of digital identity, which also includes attributes, credentials and attestations, such as age or professional qualifications, which do not necessarily identify the person but enable the provision of customized services. In certain areas, such as government services or banking, digital identity must be verified and authenticated, to prove that the person really is who they claim to be.

In a hyper-connected economy, digital identity (digID) is becoming a critical enabler of digital transactions. The need to establish individual identities uniquely, accurately, quickly and securely is not limited to individuals but extends to legal entities, machines and devices. Today, the provision of digital identity is undergoing fundamental changes as entities such as banks, providers of electronic communication services or major online platforms increasingly act as identity providers, while such market-based provision of digital identification and authentication escapes regulation.

Moreover, the COVID-19 crisis has highlighted the urgency to provide all European citizens and businesses quickly with a universally accepted, trusted digital identity and with trust services such as eSignatures to allow for seamless business continuity in the Single Market, access to crucial and sensitive public online services such as in e-Health, eGovernment and e-Justice and mitigate against identity fraud. This initiative will help to accelerate digitalisation with the aim of transforming the new dynamics experienced during the crisis into sustainable digital progress in the public and private sector.

Problem the initiative aims to tackle

The eIDAS Regulation introduced a first cross-border framework for trusted digital identities and trust services in 2014. The aim of the eIDAS regulation is to facilitate access of all EU citizens to public services across the EU by means of electronic identification (eID) issued in their home country.

Despite undisputed achievements, the potential of electronic identification and authentication under eIDAS remains underexploited. Today, only 15 of 27 Member States (~ 58% of EU population) offer cross-border eID under eIDAS to their citizens[3]. The uptake of these eID means and the offer of public online services that can be used with them is very unequal across Member States. Not all Member States offer eIDs and usage in the private sector, such as for online banking or online shopping is generally not possible as the Regulation merely encourages Member States to make eIDs available to private online service suppliers, but very few Member States have implemented this possibility. Secure and reliable market-based solutions have enjoyed some success but are not scaling up across the EU, as they operate largely in an unregulated environment[4], lacking legal certainty and incentives. Solutions of major social platforms[5] offer convenience, which comes at the cost of losing control over disclosed personal data. Moreover, these solutions are disconnected from a verified physical identity, which makes fraud (such as identity theft) and cybersecurity threats more difficult to mitigate. In addition, this practice

[2] New standards for ID cards applying as of August 2021 and providing for a contactless storage medium should provide an opportunity for more Member States to offer access to eID services using national ID cards. See: 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, OJ L 188, 12.7.2019, p. 67.

[3] The eIDAS Regulation does not oblige Member States to notify electronic identification schemes.

[4] Digital ID solutions other than publicly issued electronic IDs are not regulated in the eIDAS Regulation.

[5] "Log in with Facebook/Google/LinkedIn" that allow their users to authenticate on third-party websites and services by using their user profiles.

may raise concerns of market power and of impact on the level playing field where a competitive European digital identity user-empowering services market could develop[6].

As a result, it is not possible today to identify online with a single, secure, convenient and trustworthy eID and protect personal data as much as with an ID card or a passport in the physical world. . Despite increasing demand, available solutions do not support identification of devices, sensors, monitors, to manage their access to sensitive and non-sensitive data. Business opportunities remain untapped and secure identification costs remain excessive, such as in banking and finance, as long as trusted public eID cannot be used widely and conveniently in the private sector and/or market-based solutions are not supported by regulation.

A European identity solution enabling trusted identification of citizens and companies in their digital interactions to access public or private online services (e.g. e-commerce), should be entirely voluntary for users to adhere to and fully protect data and privacy. Anonymity of the internet should be ensured at all times by allowing solutions for anonymous authentication anonymously where user identification is not required for the provision of the service. A single trusted European ID that can be used both for public and private digital services, could boost the digitalization of the Single Market and provide a convenient single-sign-on possibility for those who wish to use it. Demand for instant, secure and convenient online transactions and evolving cyber risks drives innovation in digital identity solutions, where technologies such as AI, IoT, analytics, biometrics or mobile intersect Consequently, the extent to which the EU leads on digital ID innovation and regulation will strengthen Europe's technological autonomy and the ability of European businesses to compete globally.

Available experience with the application of eIDAS demonstrates that the Regulation carries structural shortcomings, which restrict its capability of effectively supporting a comprehensive digital ID framework. These weaknesses relate to the principle of mutual recognition in the absence of an obligation to notify, of national eID schemes, to practical difficulties in managing attributes (elements of personal information) that can be reliably disclosed to third parties, the act's focus on the public sector and the absence of possibility and/or incentives for private parties to use the national eIDs. These and other elements limiting the effectiveness of eIDAS are the subject of the ongoing evaluation of eIDAS and will be presented in parallel with the revision.

Basis for EU intervention (legal basis and subsidiarity check)

The initiative addresses the proper functioning of the Single Market for digital services (Art. 114 TFEU).

The eIDAS Regulation in its part on electronic identification is characterised by a federated system based on technological neutrality and mutual recognition binding together various digital identity solutions deployed by Member States for cross-border use. Despite the eIDAS framework, the national rules on provision of digital identity services remain fragmented in or undeveloped across the EU. Existing voluntary coordination mechanisms among Member States are not likely to bring sufficient improvement. A European digital identity that allows for a simple, trusted, secure and accessible to all public system for citizens to identify themselves and share identity related information in the digital space can be designed efficiently only at EU level. The need to ensure cross-border recognition of a digital identity system across all Member States cannot be attained by own initiatives by Member States, which vary in scope, ambition, technical architecture, retained solutions and legal arrangements,

[6] Issues pertaining to platforms will be specifically addressed in the envisaged New Competition Tool, the Digital Services Act and are a matter of data governance in general.

including liability issues and availability of use by the private sector. Individual solutions lead to fragmentation of the Single Market and encourage forum shopping by trust services providers[7], leading to unequal offering to the detriment of business opportunities, service offering and user experience.

B. Objectives and Policy options

A well-functioning Single Market for digital services enables innovation and ensures the competitiveness of the European industry. The ability to identify conveniently and securely across the internet for physical persons, companies and devices is a key condition for a seamless Single Market.

Fundamental changes in the overall societal context suggest a revision of the eIDAS Regulation. These include a dramatic increase in the use of novel technologies, such as distributed-ledger based solutions, the Internet of Things, Artificial Intelligence and biometrics, changes in market structure where few players with significant market power increasingly act as digital identity "gatekeepers", changes in user behaviour with increasing demand for instant, convenient and secure identification and the evolution of EU Data Protection legislation. The objective of this initiative is, first of all, to provide a future proof regulatory framework to support an EU-wide, simple, trusted and secure system to manage identities in the digital space, covering identification, authentication and the provision of attributes, credentials and attestations. Secondly, the initiative aims at creating a universal pan-European single digital ID.

These objectives could be achieved through an overhaul of the eIDAS system, an extension of eIDAS to the private sector, the introduction of a European Digital Identity (EUid) building on the eIDAS system or a combination of these options.

Policy options include different elements such as soft law measures (standardisation, guidelines) and different degrees of legislative intervention. These options can be combined.

In the **baseline scenario**, the eIDAS Regulation would remain unchanged. The Commission would continue assisting the Member States in complying with the mutual recognition of notified national eIDs, to the extent they are notified. The notification mechanism would remain voluntary.

Option 1 (reinforced baseline scenario) would revise and complement the existing eIDAS framework as necessary to improve coherence, consistency and interoperability. The following measures could provide additional incentives and accelerate the supply of eID schemes, extend their recognition across the public and private sectors and promote simple and secure technological solutions:

- Adoption of additional implementing acts (art. 21) and guidelines (e.g. on identity verification for issuing qualified certificates) on application of specific provisions of the eIDAS Regulation;
- Commitments by Member States to offer Digital Identity solutions and to make a step change in the digitalisation of the public sector through a strengthened digital Government Policy and an updated Tallinn declaration.[8] In addition, supplementary obligations could be introduced for Member States to implement national eID schemes or ensure citizen access by a cut-off date;[9]
- Although the eIDAS Regulation is based on the principle of technological neutrality, further harmonisation to the advantage of particularly convenient and secure solutions is possible

[7] For example, the use of biometrics (facial recognition) during user enrolment is allowed in some Member States, but firmly opposed by many others.

[8] The current EU eGovernment policy (eGovernment Action Plan) expires at the end of 2020 and needs to be reviewed. The 2017 Tallinn declaration on eGovernment by Member States could be renewed to support Member States' commitment to Digital Identity and digital Government.

[9] Several Member States grant their citizens a right to digital identity.

through requirements in implementing acts, standardisation and the introduction of certification following the Cybersecurity Act[10];

- Application of eID under eIDAS by the private sector could be promoted through guidelines on costing and liability and interoperability principles.

Option 2 consists of a more ambitious legislative intervention and would extend the scope of eID regulation under eIDAS to the private sector, notably introducing new trust services for identification, authentication and for the provision of attributes, credentials and attestations and allowing the provision of identification for devices.The introduction of requirements for digital identity providers to help enforce the provisions of the General Data Protection Regulation will be considered. In this context, digital services providers, when acting as providers of digital ID services, could be required to keep data collected for the purpose of user identification and the provision of the digital ID service separate from data generated by the user's subsequent activity on the third party service providers' website. The digital ID service provider could be precluded from using data thus generated absent explicit consent of the user, e.g. based on an opt-in clause.

Option 3 would introduce a European Digital Identity scheme (EUid) complementary with eIDAS for citizens to access online public and private services, when identification is necessary. The use of EUid would be voluntary. The introduction of requirements for online service providers to accept / recognise EUid will be considered, as well as requirements for Member States to ensure general availability and access to eID and to make notification of national eID schemes under eIDAS mandatory.

C. Preliminary Assessment of Expected Impacts [max 20 lines]

Baseline scenario – no EU policy change

In the baseline scenario, the eIDAS Regulation would remain unchanged.

The Commission would continue assisting the Member States in complying with the mutual recognition of notified national eIDs, to the extent that the Member States notify and the notification mechanism would remain voluntary.

This scenario would most likely not deliver swift progress in providing access to eID for all citizens, it would not cover legal entities and devices and not assist an extension of eID under eIDAS to the private sector. Private sector providers, and especially online platforms, would increasingly provide identification services with little or no effective consumer choice to decide over the use of significant amount of disclosed data and to protect privacy when identifying online. The fight against identity theft and cybersecurity threats would not be facilitated.

Likely economic impacts

Compared to the baseline scenario, all options are expected to improve to varying extent the supply of and demand for digital ID means, reducing transaction costs for the identification, authentication and regulatory compliance in certain sectors (e.g. customer enrolment in the banking sector) and creating new business opportunities. An extension of eIDAS to the private sector is likely to generate considerable economic gains through an increased offer and uptake of identification and authentication for activities intermediated online[11]. EU-based SMEs and digital service innovators in particular are expected to be the main beneficiaries of the economic gains.

[10] Regulation 2019/881

[11] According to a McKinsey report from January 2019, digital identity has considerable potential for wealth creation. In mature economies, the average country could achieve economic value equivalent to roughly 3 percent—both assuming high levels of adoption and use in multiple domains (https://mck.co/2UvbmN9)

Option 1 would have a positive, albeit limited, economic effect through guidelines promoting the extension of eID under eIDAS to the private sector.

Option 2 entails an extension of the eIDAS framework to the private sector and an extension of the catalogue of trust services. As such, this option would tackle many of the shortcomings of the currently applicable eIDAS Regulation. This legislative intervention would likely achieve a positive impact for digital identity services by providing more options for the market and clarified, uniform and better adapted rules. This option promises most impact on competitiveness and innovation as it significantly opens the eIDAS system to new trust services and extends its scope to devices paving the way for innovative digital ID means service providers. It would also support emerging use cases that require trustworthy personal information, such as those in the financial sector. The framework would enable different modalities of identification provision, including unverified identities, anonymous identities but subject to identity verification and verified identities with full disclosure of identification data. However, the option could not realise its benefits without the accompanying non-legislative measures such as standardisation or guidelines.

Option 3: The introduction of a European Digital Identity scheme (EUid) together with requirements for recognition, notification and access is likely to have a significant impact regarding distribution, access and usability of eID under eIDAS. Alone, and depending on the method of implementation, it may however fall short of addressing many the shortcomings of the eIDAS Regulation, such as the absence of a predictable and uniform regulatory framework for privately supplied digital ID solutions.

The highest economic impact is probably to be expected from the combination of all three options, correcting the weaknesses of the eIDAS regulation (option 1), extending its reach to the private sector (option 2) and creating a universally accepted EUid (option 3). This combination would also probably be most effective in tackling current shortcomings as well as extending the offer and uptake leading to most gains further in the value chain for users of digital ID means (citizens and businesses). Options 2 and 3 would also provide an opportunity for the public sector to stimulate innovation via its procurement role for digital public services.

An extension of the eID regulation to the private sector would incur some compliance costs to identity providers. However, considerably higher benefits would be created with new business opportunities through the creation of new trust services for identification, authentication and provision of attributes and by enabling eID for legal entities and devices. Possible costs associated with requirements for digital identity providers to enforce data protection principles (e.g. separate identity and activity data) would be offset by the benefits created by facilitating GDPR-compliance regarding enabling purpose limitation, minimisation of data collection and disclosure and the expression of consent. While some compliance costs would be incurred by online service providers ensuring recognition for EUid (option 3), standardised interfaces and the interoperability framework would simplify this and economic benefits would be created through the opportunity to identify / authenticate through trusted means, in particular in specific sectors (e.g. banking and finance) (option 2).

In addition, creation of business opportunities and private sector cost reduction is one of the guiding principles of the options proposed.

Requirements for Member States to ensure general access to eID and to make notification of national eID schemes under eIDAS mandatory could incur costs to Member States depending on the stage of development of national eID systems. Options 2 and 3 would also promote the digitalisation of public services and improve cybersecurity, increasing efficiency and reducing public expenditure.

Likely social impacts

Options 2 and 3 offer considerable positive social impacts as they create consumer choices for trusted digital ID that can be used across the internet while ensuring data protection and privacy. The possibility for the user to actively manage attributes, credentials and attestations (e.g. gender, age, professional qualification etc.) would empower user control of digital identity and enable personalised

online services in a trusted environment where online privacy can be ensured and data is protected. This represents a considerable social benefit compared to the current situation.

The opportunities created by EUid also include better access to services, more customized digital experiences, better protection against identity fraud and reduced cybersecurity threats. Improving user choice in digital identification would safeguard long-term consumer interests and social welfare.

Likely environmental impacts

Environmental impacts are marginal for Option 1, compared with the baseline. For other options, increased use of online services may lead to an increase in the net computation expenditure, which could have an impact on the carbon footprint of the public and private digital services sector. This impact, however, might be compensated by reduced transportation carbon footprint brought by the substitution of face-to-face interactions with remote interactions. Also, enhanced digital identity solutions would improve traceability in supply chains for the benefit of global biodiversity protection. Given the variety of sectors, the environmental implications could be diverse and the Impact Assessment would need to analyse them in more detail.

Likely impacts on fundamental rights

Option 1 would only have marginal impact on fundamental rights.

All other options would exert a positive impact on personal data protection and privacy as it would increase the offer of digital identity means empowering consumers and business to manage and protect their own data and privacy. Digital services, enabled by eID, support fundamental rights and the rule of law, as they offer a level of resilience to social and justice systems in times of crisis. In addition, Option 2 in particular would create opportunities to empower refugees, stateless and forcibly displaced persons by making it possible to grant them digital identities in absence of analogue documents issued by the authorities of their state of origin.

Option 3 would create positive impact on data protection by way of imposing a clear separation between the collection of personal identity data and the collection of other data for commercial exploitation.

Likely impacts on simplification and/or administrative burden

Increased efficiency of the eIDAS framework and a better offer and uptake of public and private eID as it is pursued to different degree by all options, save for the baseline option, are likely to significantly reduce the administrative burden of public and private service providers. Offering a widely usable digital alternative to current paper-based identification would bring significant efficiency gains and boost digital transformation of public and private services. Expected impact is significant as demonstrated by the example of a Member State where digital ID is ubiquitous[12].

The use of secure and reliable digital identification by the providers of various digital services would support their compliance with various regulatory requirements (e.g. GDPR, privacy), particularly in those sectors where identification of the customers is regulated by law.

Whereas options 2 and 3 are expected to create some compliance costs to private sector identity providers, and would require investment by Member States, it is very likely that these costs would be more than counterbalanced by the return on investments created by new business opportunities, significant efficiency gains and a wider accessibility of digital public services.

[12] Estonia estimates that digital ID under the eIDAS framework has contributed to saving 1407 years of working time, enabling over 900 million transactions a year in a country of 1.3 million, full automatisation in tax-reporting, a few hours only to start a company, 99% of state services available also digitally 24/7

Highest initial compliance costs to the public sector would be incurred by options 2 and 3 but those would also lead to administrative simplification and the reduction of administrative burden across the EU and deliver long-term cost savings for public administrations.

D. Evidence Base, Data collection and Better Regulation Instruments

Impact Assessment

The initiative will build on the results of the ongoing review of the eIDAS Regulation, which is linked to the regulatory obligation for review included in Article 49 of the Regulation.

A study to support the Impact Assessment was launched in Q2 2020. An evaluation and evaluation study will also contribute data, views and evidence.

An Inter-Service Group including all relevant Commission services has been created to advise the process of evaluation and impact assessment.

Evidence base and data collection

Qualitative and quantitative data gathered by the study to support the evaluation of eIDAS and the study to support the IA of the options for the revision of eIDAS will be used in the impact assessment.

Both impact assessment and evaluation will be informed by a single open public consultation published in Q3 2020. A targeted stakeholder consultation and interviews will complete the open public consultation. A stakeholder workshop will be held in Q3 2020.

Consultation of citizens and stakeholders

The aims of the consultation are:

1. to collect views, data and evidence on the implementation of the eIDAS Regulation to inform the eIDAS review; and
2. to collect views, data and evidence on the impacts of the alternatives for delivering an EU digital identity in order to support the Commission's assessment and choice of regulatory option for this initiative.

Planned consultation activities:

- Open Public Consultation, 10 weeks, all EU languages. The launch of stakeholder consultations related to this initiative will be announced in the consultation planning that can be found at *http://ec.europa.eu/yourvoice/consultations/docs/planned-consultations_en.pdf.*
- Targeted stakeholder interviews organised by the Commission with selected experts on different aspects of digital identity

With regard to **the eIDAS review**, the consultation will cover all five evaluation criteria (effectiveness, efficiency, consistency, relevance, EU-added value), identify gaps, challenges and opportunities and inform how to remedy gaps or challenges or build on opportunities. Stakeholders will also be asked to share views and evidence on the costs and benefits of the current eIDAS operating model.

With regard to the **revision of the eIDAS Regulation**, the consultation will cover cost/benefit analyses for the options and their components. In addition, the consultation will cover aspects such as likely impacts on simplification and/or administrative burden, SME's, competitiveness and innovation, public administration, governance and supervision, international trade, technological autonomy as well as societal and environmental impacts of the various options.

Targeted stakeholder consultation activities will include a focus on the main technological and market development trends affecting online trust services, including the emergence of more decentralised forms of trust services (Distributed Ledger Technologies, such as blockchain). In addition, they will cover different technological means for implementing a digital ID solution, from hardware (smart cards) to mobile solutions, with related aspects such as the use of biometrics and the related security vs. convenience aspects.

Will an Implementation plan be established?
x Yes ☐ No