063468/EU XXVII.GP
Eingelangt am 03/06/21

EUROPEAN
COMMISSION

Brussels, 3.6.2021
COM(2021) 281 final

2021/0136 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

www.parlament.gv.at

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This explanatory memorandum accompanies the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)[1]. The legal instrument aims to provide, for cross-border use:

– access to highly secure and trustworthy electronic identity solutions,

– that public and private services can rely on trusted and secure digital identity solutions,

– that natural and legal persons are empowered to use digital identity solutions,

– that these solutions are linked to a variety of attributes and allow for the targeted sharing of identity data limited to the needs of the specific service requested,

– acceptance of qualified trust services in the EU and equal conditions for their provision.

What is emerging in the market 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. There is an increased demand for electronic identity solutions that can deliver these capabilities providing efficiency gains and a high level of trust across the EU, both in the private and the public sector, relying on the need to identify and authenticate users with a high level of assurance.

The evaluation of the eIDAS Regulation[2] revealed that the current Regulation falls short of addressing these new market demands, mostly due to its inherent limitations to the public sector, the limited possibilities and the complexity for online private providers to connect to the system, its insufficient availability of notified eID solutions in all Member States and its lack of flexibility to support a variety of use cases. Furthermore, identity solutions falling outside the scope of eIDAS, such as those offered by social media providers and financial institutions, raise privacy and data protection concerns. They cannot effectively respond to new market demands and lack the cross border outreach to address specific sectoral needs where identification is sensitive and requires a high degree of certainty.

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. As a result, only 59 % of EU residents have access to trusted and secure eID schemes across borders. Only 7 schemes are entirely mobile, responding to current user expectations. As not all technical nodes to ensure the connection to the eIDAS interoperability framework are fully operational, cross-border access is limited; very few online public services accessible domestically can be reached cross-border via the eIDAS network.

---

1 OJ L 257/73 of 28.8.2014

2 [add reference once adopted]

www.parlament.gv.at

By offering a European Digital Identity framework based on the revision of the current one, at least 80% of citizens should be able to use a digital ID solution to access key public services by 2030. Furthermore, the security and control offered by the European Digital Identity framework should give citizens and residents full confidence that the European Digital Identity framework will offer everyone the means to control who has access to their digital twin and to which data exactly. This will also require a high level of security with respect to all aspects of digital identity provisioning, including the issuing of a European Digital Identity Wallet, and the infrastructure for the collection, storage and disclosure of digital identity data.

Furthermore, the current eIDAS framework does not cover the provision of electronic attributes, such as medical certificates or professional qualifications, making it difficult to ensure pan-European legal recognition of such credentials in electronic form. In addition, the eIDAS Regulation does not allow users to limit the sharing of identity data to what is strictly necessary for the provision of a service.

While the evaluation of the eIDAS Regulation shows that the framework for the provision of trust services has been rather successful, providing a high level of trust and ensuring the uptake and use of most trust services, more needs to be done to reach full harmonisation and acceptance. For qualified certificates of website authentication, citizens must be able to rely on them and benefit from the secure and trustworthy information about who is behind a web site, thus reducing fraud.

In addition, to respond to the dynamics of the markets and to technological developments, this proposal expands the current eIDAS list of trust services with three new qualified trust services, namely the provision of electronic archiving services, electronic ledgers and the management of remote electronic signature and seal creation devices.

This proposal also offers a harmonised approach to security, for citizens relying on a European digital identity representing them online, and for online service providers who will be able to fully rely on and accept digital identity solutions independently of where they have been issued. This proposal implies a shift for issuers of European digital identity solutions, providing a common technical architecture and reference framework and common standards to be developed in collaboration with the Member States. A harmonised approach is necessary to avoid that the development of new digital identity solutions in Member States create further fragmentation triggered by the use of divergent national solutions. A harmonised approach will also strengthen the Single Market as it would allow citizens, other residents and businesses to identify online in a secure, convenient and uniform way across the EU to access both public and private services. Users would be able to rely on an improved ecosystem for electronic identity and trust services recognised and accepted everywhere in the Union.

In order to avoid fragmentation and barriers due to diverging standards, the Commission will adopt a Recommendation at the same time as this proposal. This Recommendation will setout a process to support a common approach allowing Member States and other relevant stakeholders from the public and private sectors, in close coordination with the Commission, to work towards the development of a Toolbox to avoid divergent approaches and avoid endangering the future implementation of the European Digital Identity framework.

- **Consistency with existing policy provisions in the policy area**

This proposal builds on the current eIDAS Regulation, on the role of Member States as providers of legal identities and on the framework for the provision of electronic trust services in the European Union. The proposal is complementary and fully coherent with other policy

www.parlament.gv.at

instruments at EU level aiming to translate the benefits of the internal market in the digital world, particularly by increasing the possibilities for citizens to access services cross-border. In this respect, the proposal implements the political mandate provided by the European Council[3] and the President of the European Commission [4]to provide an EU-wide framework for public electronic identities which ensures that any citizen or residents can have access to a secure European e-identity, which can be used anywhere in the EU to identify and authenticate for access to services in the public and private sectors, allowing citizens to control what data is communicated and how it is used.

- **Consistency with other Union policies**

The proposal is consistent with the priorities for the digital transformation as set out in the strategy Shaping Europe's Digital Future[5] and will support achieving the targets indicated in the Digital Decade Communication[6]. Any personal data processing under this Regulation should be carried out in full compliance with the General Data Protection Regulation (now onwards GDPR)[7]. In addition, this Regulation introduces specific data protection safeguards.

To ensure a high level of security, the proposal is also consistent with Union policies related to cyber security[8]. The proposal has been designed to reduce fragmentation applying the general cyber security requirements to trust service providers regulated by the eIDAS Regulation.

This proposal is furthermore coherent with other sectorial policies relying on the use of electronic identities, electronic attestations of attributes and other trust services. This includes the Single Digital Gateway Regulation[9], requirements to be fulfilled in the financial sector related to anti money laundering and counter terrorism financing, initiatives to share social security credentials, for a digital driving licence or for future digital travel documents and other initiatives set out to reduce administrative burden for citizens and businesses relying fully on the possibilities provided by the digital transformation of procedures both in the public and the private sector. The wallet will furthermore enable qualified electronic signatures that can facilitate political participation[10].

---

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

4 State of the Union speech 16 September 2020, see https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Shaping Europe's digital future

6 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1

8 https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

9 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, 21.11.2018, p. 1

10 European Democracy Action Plan, COM/2020/790 final.

www.parlament.gv.at

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

This initiative aims to support the Union's transformation towards a Digital Single Market. With the growing digitisation of cross-border public and private services which rely on the use of digital identity solutions, there is a risk that within the current legal framework, citizens will continue to face obstacles and not be able to make full use of online services seamlessly throughout the EU and to preserve their privacy. 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.

• Subsidiarity (for non-exclusive competence)

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 from the portability of electronic attestations of attributes linked to identity. Recent technological developments, market and user demand require the availability of more user friendly cross border solutions that allow access to online services EU–wide, which the eIDAS Regulation in its current form cannot offer.

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 market power of large providers, which requires interoperability and trusted eIDs at EU level. In addition, electronic attestations of attributes issued and accepted in one Member State, such as an electronic health certificate, are often not legally recognised and accepted in other Member States. This creates the risk that Member States continue to develop fragmented national solutions that cannot operate across borders.

For the provision of Trust Services, although largely regulated and functioning in accordance with the current legal work, national practices also create the risk of increased fragmentation.

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, in compliance with EU data protection rules. 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 harmonised conditions that ensure user control and access to cross border online digital services and an interoperability framework making it easy for online services to rely on the use of secure digital identity solutions, irrespective of where in the EU it has been issued or where a citizen resides. As largely reflected in the review of the eIDAS Regulation, it is unlikely that national intervention would be equally efficient and effective.

• Proportionality

This initiative is proportionate to the objectives sought, providing an 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 on the provision of qualified and non-qualified digital identity attributes. It provides a clear contribution to the objective of improving the Digital Single Market through a more harmonised legal framework. The harmonised European digital Identity wallets to be issued by the Member States on the basis of common technical standards also provide a common EU approach benefitting users and parties relying on the availability of secure cross-border electronic identity solutions. This initiative addresses the limitations of the current electronic identification interoperability infrastructure based on mutual recognition of diverse national

www.parlament.gv.at

electronic identification schemes. Taking into consideration the set objectives, this initiative is considered sufficiently proportionate and the costs likely to be commensurate to the potential benefits. The proposed Regulation will give rise to financial and administrative costs, which are to be borne by Member States as issuers of the European Digital Identity wallets, by trust services and online service providers. However, these costs would likely be outweighed by the significant potential benefits for citizens and users stemming directly from an increase in cross-border recognition and acceptance of electronic identity and attribute services.

The costs derived from creating and aligning to the new standards for trust service providers and online service providers cannot be avoided if the objective of usability and accessibility is to be achieved. The initiative intends to harness and build on the investment already made by Member States in their national identity schemes. Furthermore, the additional costs generated by the proposal are designed to support harmonisation and justified on the expectation that, in the long run, they will reduce administrative burden and compliance costs. 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.

- **Choice of the instrument**

The choice of a regulation as the legal instrument is justified by the need to ensure uniform conditions in the Internal Market for the application of the European Digital Identity by means of a harmonised framework that aims to create seamless interoperability and provide European citizens and companies with public and private services across the Union with highly secure and trustworthy eIDs.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

An evaluation of the functioning of the eIDAS Regulation was conducted as part of the review process required by Article 49 of the eIDAS Regulation. The main findings of the evaluation with respect to electronic identity is that eIDAS has not achieved its potential. Only a limited number of eIDs have been notified, limiting the coverage of notified eID schemes to about 59% of EU population. In addition, the acceptance of notified eIDs both at the level of Member States and service providers is limited. It also appears that only a few of the services accessible through domestic eID are connected to the national eIDAS infrastructure. The evaluation study has also found that the current scope and focus of the eIDAS Regulation on eID schemes notified by EU Member States and on enabling access to online public services seems too limited and inadequate. The vast majority of the needs of electronic identity and remote authentication remain with the private sector, in particular in areas like banking, telecom and platform operators that are required by law to verify the identity of their customers. The added value of the eIDAS Regulation with regard to electronic identity is limited due to its low coverage, uptake and usage.

The problems identified in this proposal are linked to the shortcoming of the current eIDAS framework and fundamental contextual changes regarding markets, societal and technological developments triggering new user's and market's needs.

www.parlament.gv.at

- **Stakeholder consultations**

An open public consultation was launched on 24 July 2020 and closed on 02 October 2020. In total, the Commission received 318 contributions. The Commission also received 106 replies to a targeted stakeholder survey. Opinions have also been gathered from Member States in a variety of bilateral and multilateral meetings and surveys organised since early 2020. This notably includes a survey of Member State representatives of the eIDAS Cooperation Network in July-August 2020 and various dedicated workshops. The Commission also held in-depth interviews with industry representatives and met business stakeholders in various sectors (e.g. eCommerce, health, financial services, telecom operators, equipment manufacturers etc.) in bilateral meetings.

A large majority of respondents to the open public consultation welcomed the creation of a single and universally accepted digital identity relying on the legal identities issued by Member States. Member States largely support the need to reinforce the current eIDAS Regulation providing citizens with the possibility to access both public and private services and recognise the need to establish a trust service allowing for the issuing and cross-border use of electronic attestations of attributes. Overall, Member States emphasized the need to build a European Digital Identity Framework on the experience and strength of the national solutions, seeking to find synergies and benefitting from investments made. Many stakeholders referred to how the COVID-19 pandemic had demonstrated the value of secure, remote identification for all to access public and private services. On trust services, most actors agree that the current framework has been a success, however, some additional measures were required to further harmonise certain practices related to remote identification and national supervision. Stakeholders with a largely national customer base expressed more doubts about the added value of a European Digital Identity framework.

Digital identity wallets are perceived more and more by the public and private sector as the most appropriate instrument allowing users to choose when and with which private service provider to share various attributes, depending on the use case and the security needed for the respective transaction. Digital identities based on digital wallets stored securely on mobile devices were identified as a main asset for a future-proof solution. Both the private market (e.g. Apple, Google, Thales) and governments already move in this direction.

- **Collection and use of expertise**

The proposal is based on the information collected as part of the stakeholder consultation for the purpose of the impact assessment and evaluation reports of the eIDAS Regulation in view of the review obligations set out in Article 49 of the eIDAS Regulation. Numerous meetings have been organised with Member State representatives and experts.

- **Impact assessment**

An impact assessment was carried out for this proposal. On 19 March 2021, the Regulatory Scrutiny Board issued a negative opinion with some comments. Following a revised resubmission, on 5 May 2021, the Board delivered a positive opinion.

The Commission examines different policy options to achieve the general objective of the present initiative, which is to ensure the proper functioning of the internal market, particularly in relation to the provision and use of highly secure and trustworthy electronic identity solutions.

www.parlament.gv.at

The impact assessment examines the baseline scenario, policy options and their impacts for the three policy options considered. Each option presents a choice for political consideration based on the level of ambition. The first option presents a low level of ambition and a set of measures mainly aiming to strengthen the effectiveness and efficiency of the current eIDAS Regulation. By imposing mandatory notification of national eIDs and streamlining the existing instruments available to achieve mutual recognition, the first option is based on meeting the needs of citizens by relying on the availability of diverse national eID schemes that aim to become interoperable.

The second option presents a medium ambition level and mainly aims to extend the possibilities for the secure exchange of data linked to identity, complementing government eIDs and supporting the current shift towards attribute based identity services. The aim of this option would have been to meet user demand and create a new qualified trust service for the provision of electronic attestations of attributes linked to trusted sources and enforceable cross-border. This would have extended the scope of the current eIDAS Regulation and supported as many use cases as possible relying on the need to verify identity attributes linked to a person with a high level of assurance.

The third and preferred option presents the highest level of ambition and aims to regulate the provision of a highly secure personal digital identity wallet issued by Member States. The preferred option was considered to address in the most effective way the objectives of this initiative. To fully address the policy objectives, the preferred option builds on most measures assessed under option one (reliance on legal identities attested to by Member States and the availability of mutually recognised eID means) and option two (electronic attestations of attributes legally recognised cross border).

With regards to the general framework for Trust Services, the level of ambition calls for a set of measures not requiring a step-wise approach in order to meet the policy objectives.

The new qualified trust service for the management of remote electronic signature and seal creation devices would bring considerable security, uniformity, legal certainty and consumer choice benefits both linked to the certification of the qualified signature creation devices and in relation to the requirements to be fulfilled by the qualified trust service providers managing such devices. The new provisions would reinforce the overall regulatory and supervision framework for trust service provision.

The impacts of the policy options on different categories of stakeholders are explained in details in Annex 3 of the Impact Assessment supporting this initiative. The assessment is both quantitative and qualitative. The Impact assessment study indicates that the minimum quantifiable costs can be estimated at €3.2+ billion, since some of the cost items cannot be quantified. Total quantifiable benefits have been estimated to € 3.9 billion – 9.6 billion. With regards to the wider economic impacts, the preferred option is expected to have a positive impact on innovation, international trade and competitiveness, contribute to economic growth and lead to additional investment in digital identity solutions. For example an additional € 500 million investment triggered by the legislative changes under option 3 is expected to generate benefits of € 1,268 million after 10 years (at 67% adoption).

The preferred option is also expected to generate a positive impact on employment, generating between 5,000 and 27,000 additional jobs over the 5 years following the implementation. This is explained by the additional investment and the reduced costs for businesses relying on the use of eID solutions.

www.parlament.gv.at

The positive environmental impact is expected to be greatest for the third option, which is expected to improve to the maximum extent the take up and usability of eID, bringing positive impacts on the emissions reduction related to public service delivery.

Electronic ledgers provide users with proof and an immutable audit trail for the sequencing of transactions and data records, safeguarding data integrity. While this trust service was not part of the impact assessment, it builds upon existing trust services as it combines time stamping of data and their sequencing with certainty about the data originator, which is similar to e-signing. This trust service is necessary to prevent fragmentation of the internal market, by defining a single pan-European framework that enables the cross-border recognition of trust services supporting the operation of qualified electronic ledgers. Data integrity, in turn, is very important for the pooling of data from decentralised sources, for self-sovereign identity solutions, for attributing ownership to digital assets, for recording business processes to audit compliance with sustainability criteria and for various use cases in capital markets.

- **Regulatory fitness and simplification**

This proposal lays down measures that will apply to public authorities, citizens and online service providers. It will reduce administrative and compliance cost for public administrations and operational costs and reduced expenditure related to security for online service providers. Citizens will benefit from savings from reduced administrative burden, relying fully on digital means to identify and the facility to securely exchange digital identity attributes with the same legal value cross border. Electronic identity providers will also benefit from savings in compliance costs.

- **Fundamental rights**

Since personal data falls within the scope of some elements of the Regulation, the measures are designed to fully comply with the data protection legislation. For example, the proposal improves options to share data and to enable discretional disclosure. Using the European Digital Identity Wallet, the user will be able to control the amount of data provided to relying parties and be informed about the attributes required for the provision of a specific service. Service providers shall inform Member States of their intention to rely on a European Digital Identity Wallet, which would allow Member States to control that sensitive data sets, for example, related to health are only requested by service providers in accordance with national law.

4. BUDGETARY IMPLICATIONS

In order to optimally achieve the objectives of this initiative, it is necessary to finance a number of actions both at the Commission level, where the allocation of about 60 FTEs is envisaged in the period 2022-2027 and at Member State level through their active participation in the expert groups and committees linked with the work of the initiative and which are composed of the representatives of Member States. The total financial resources necessary for the implementation of the proposal in the 2022-2027 period will be up to EUR 30.825 million, including EUR 8.825 million of administrative costs and up to EUR 22 million in operational spending covered by the Digital Europe Programme (pending agreement). The financing will support costs linked to maintaining, developing, hosting, operating and supporting the eID and trust services' building blocks. It may also support grants for connecting services to the European Digital Identity Wallet ecosystem, the development of standards and technical specifications. Finally, financing will also support carrying out annual surveys and studies effectiveness and the efficiency of the regulation in

www.parlament.gv.at

reaching its objectives. The "financial statement" linked to this initiative provides a detailed overview of the costs involved.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The impacts will be monitored and evaluated in accordance with the Better Regulation Guidelines covering the implementation and application of the proposed Regulation. The monitoring arrangement constitutes an important part of the proposal, in particular in view of the shortcomings of the current reporting framework, as shown by the evaluation study. In addition to the reporting requirements introduced in the proposed Regulation, which aim to ensure a better data and analysis base, the monitoring framework will monitor: 1) the extent to which the necessary changes have been implemented in line with the adopted measures; 2) whether the necessary changes to the relevant national systems have been implemented; 3) whether the necessary changes to the compliance obligations by the regulated entities have been adhered to. The European Commission (1, 2 and 3) and the National Competent Authorities (2 and 3) will be responsible for the data collection based on pre-defined indicators.

On the application of the proposed instrument, the European Commission and the National Competent Authorities will assess through annual surveys: 1) the access to eID means for all EU citizens; 2) the increased cross-border recognition and acceptance of eID schemes; 3) measures to stimulate the adoption by the private sector and the development of new digital identity services.

Contextual information will be gathered by the European Commission using annual surveys on: 1) the size of the market for digital identities; 2) public procurement expenditure linked to digital identity; 3) share of businesses providing their services online; 4) share of online transactions requiring strong customer identification; 5) share of EU citizens using online private and public services.

- **Detailed explanation of the specific provisions of the proposal**

The draft Regulation requires Member States in Article 6a to issue a European Digital Identity Wallet under a notified eID scheme to common technical standards following compulsory compliance assessment and voluntary certification within the European cybersecurity certification framework, as established by the Cybersecurity Act. It includes provisions to ensure that natural and legal persons shall have the possibility to securely request and obtain, store, combine and use person identification data and electronic attestations of attributes to authenticate online and offline and to allow access to goods and online public and private services under the user's control. This certification is without prejudice to the GDPR in the meaning that personal data processing operations relating to the European Digital Identity wallet can only be certified pursuant to Articles 42 and 43 GDPR.

The proposal sets out in Article 6b specific provisions on the requirements applicable to relying parties for the prevention of fraud and to ensure the authentication of personal identification data and electronic attestations of attributes originating from the European Digital Identity Wallet.

For the purpose of making more electronic identification means available for cross border use and improving the efficiency of the process of mutual recognition of notified electronic identification schemes, the notification of at least one electronic identification scheme by

www.parlament.gv.at

Member States is made mandatory in Article 7. In addition, provisions to facilitate unique identification are added to ensure the unique and persistent identification of natural persons in Article 11a. This concerns cases where identification is required by law such as in the area of health, in the area of finance to discharge anti-money laundering obligations, or for judicial use. For this purpose, Member States will be required to include a unique and persistent identifier in the minimum set of person identification data. The possibility for Member States to rely on certification to ensure conformity with the Regulation and thereby replacing the process of peer review, improves the efficiency of mutual recognition.

Section 3 presents new provisions on the cross-border reliance on the European Digital Identity Wallet to ensure that users can rely on the use of European Digital Identity Wallets to access online services provided by public sector bodies and by private service providers requiring the use of strong user authentication.

In Chapter III on trust services, Article 14 on International aspects is amended to allow the Commission the possibility of adopting implementing decisions attesting the equivalence of the requirements applied to trust services established in third countries and of the services they provide, in addition to the use of mutual recognition agreements in accordance with Article 218 TFEU.

Regarding the general provision applicable to trust services, including qualified trust service providers, Articles 17, 18, 20, 21 and 24 are amended to align with the rules applicable to Network and Information Security in the EU. When it comes to the methods to be used by qualified trust service providers to verify the identity of the natural or legal persons to whom the qualified certificates are issued, the provisions on the use of remote means of identification have been harmonised and clarified in order to ensure that the same rules are applied across the EU.

Chapter III presents a new article 29a to define requirements for a qualified service for the management of remote electronic signature creation devices. The new qualified trust service would be directly linked and build on measures referenced and assessed in the impact assessment notably measures on the “Harmonisation of the certification process for remote electronic signing” and other measures calling for the harmonisation of supervision practices by Member States.

In order to ensure that users can identify who is behind a website, Article 45 is amended to require providers of web browsers to facilitate the use of qualified certificates for website authentication.

Chapter III presents three new sections.

The new section 9 inserts provisions on the legal effects of electronic attestations of attributes, their use in defined sectors and the requirements for qualified attestations of attributes. In order to ensure a high level of trust, a provision on the verification of attributes against authentic sources is inserted in Article 45d. To make sure that users of the European Digital Identity Wallet can benefit from the availability of electronic attestations of attributes and have such attestations issued to the European Digital Identity Wallet, a requirement is inserted in Article 45e. Article 45f contains, instead, additional rules for the provision of electronic attestation of attribute services, including on the protection of personal data.

The new section 10 allows for the provision of qualified electronic archiving services at the EU level. Article 45g on qualified electronic archiving services complements Articles 34 and 40 on qualified preservation services for qualified electronic signatures and qualified electronic seals.

www.parlament.gv.at

The new section 11 establishes a framework for trust services in regards to the creation and maintenance of electronic ledgers and qualified electronic ledgers. An electronic ledger combines time stamping of data and their sequencing with certainty about the data originator similar to e-signing with the additional benefit of enabling a more decentralized governance that is suitable for multi-party cooperation. This is important for various use-cases that can be built on electronic ledgers.

Electronic ledgers help companies saving costs by making multiparty coordination more efficient, safer and they facilitate regulatory supervision. In the absence of European regulation, there is a risk that national legislators will set diverging national standards. To prevent fragmentation, it is necessary to define a single pan-European framework that will enable the cross-border recognition of trust services supporting the operation of electronic ledgers. This pan-European standard for node operators will apply notwithstanding other EU secondary legislation. Where electronic ledgers are used to support the issuing and/or trading of bonds, or for crypto assets, use cases should be compatible with all applicable financial rules for example with the Markets in Financial Instruments Directive[11], the Payment Services Directive[12] and the future Markets in Crypto Assets Regulation[13]. Where use cases involve personal data, service providers will need to comply with the GDPR.

75% of all use cases for electronic ledgers were in banking and finance back in 2017. Use cases for electronic ledgers are today increasingly diverse, with 17% in communication & media; 15% in manufacturing & natural resources, 10% in the governmental sector, 8% in insurance, 5% in retail, 6% in transportation, 5% in utilities[14].

Finally, chapter VI has a new Article 48b to ensure that statistics on the use of the European Digital Identity Wallet is collected for monitoring the effectiveness of the amended Regulation.

---

11 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance, *OJ L 173, 12.6.2014, p. 349–496.*

12 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, *OJ L 337, 23.12.2015, p. 35–127.*

13 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final.

14 Gartner, Blockchain Evolution, 2020.

www.parlament.gv.at

2021/0136 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[15],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Commission Communication of 19 February 2020, entitled "Shaping Europe's Digital Future"[16] announces a revision of Regulation (EU) No 910/2014 of the European Parliament and of the Council with the aim of improving its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.

(2) In its conclusions of 1-2 October 2020[17], the European Council called on the Commission to propose the development of a Union-wide framework for secure public electronic identification, 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.

(3) The Commission Communication of 9 March 2021 entitled "2030 Digital Compass: the European way for the Digital Decade"[18] sets the objective of a Union framework which, by 2030, leads to wide deployment of a trusted, user-controlled identity, allowing each user to control their own online interactions and presence.

(4) A more harmonised approach to digital identification should reduce the risks and costs of the current fragmentation due to the use of divergent national solutions and will strengthen the Single Market by allowing citizens, other residents as defined by national law and businesses to identify online in a convenient and uniform way across the Union. Everyone should be able to securely access public and private services relying on an improved ecosystem for trust services and on verified proofs of identity and attestations of attributes, such as a university degree legally recognised and

15 OJ C , , p. .

16 COM/2020/67 final

17 https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

18 COM/2021/118 final/2

www.parlament.gv.at

accepted everywhere in the Union. The framework for a European Digital Identity aims to achieve a shift from the reliance on national digital identity solutions only, to the provision of electronic attestations of attributes valid at European level. Providers of electronic attestations of attributes should benefit from a clear and uniform set of rules and public administrations should be able to rely on electronic documents in a given format.

(5) To support the competitiveness of European businesses, online service providers should be able to rely on digital identity solutions recognised across the Union, irrespective of the Member State in which they have been issued, thus benefiting from a harmonised European approach to trust, security and interoperability. Users and service providers alike should be able to benefit from the same legal value provided to electronic attestations of attributes across the Union.

(6) Regulation (EU) No 2016/679[19] applies to the processing of personal data in the implementation of this Regulation. Therefore, this Regulation should lay down specific safeguards to prevent providers of electronic identification means and electronic attestation of attributes from combining personal data from other services with the personal data relating to the services falling within the scope of this Regulation.

(7) It is necessary to set out the harmonised conditions for the establishment of a framework for European Digital Identity Wallets to be issued by Member States, which should empower all Union citizens and other residents as defined by national law to share securely data related to their identity in a user friendly and convenient way under the sole control of the user. Technologies used to achieve those objectives should be developed aiming towards the highest level of security, user convenience and wide usability. Member States should ensure equal access to digital identification to all their nationals and residents.

(8) In order to ensure compliance within Union law or national law compliant with Union law, service providers should communicate their intent to rely on the European Digital Identity Wallets to Member States. That will allow Member States to protect users from fraud and prevent the unlawful use of identity data and electronic attestations of attributes as well as to ensure that the processing of sensitive data, like health data, can be verified by relying parties in accordance with Union law or national law.

(9) All European Digital Identity Wallets should allow users to electronically identify and authenticate online and offline across borders for accessing a wide range of public and private services. Without prejudice to Member States' prerogatives as regards the identification of their nationals and residents, Wallets can also serve the institutional needs of public administrations, international organisations and the Union's institutions, bodies, offices and agencies. Offline use would be important in many sectors, including in the health sector where services are often provided through face-to-face interaction and ePrescriptions should be able to rely on QR-codes or similar technologies to verify authenticity. Relying on the level of assurance "high", the European Digital Identity Wallets should benefit from the potential offered by tamper-proof solutions such as secure elements, to comply with the security requirements

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1

www.parlament.gv.at

under this Regulation. The European Digital Identity Wallets should also allow users to create and use qualified electronic signatures and seals which are accepted across the EU. To achieve simplification and cost reduction benefits to persons and businesses across the EU, including by enabling powers of representation and e-mandates, Member States should issue European Digital Identity Wallets relying on common standards to ensure seamless interoperability and a high level of security. Only Member States' competent authorities can provide a high degree of confidence in establishing the identity of a person and therefore provide assurance that the person claiming or asserting a particular identity is in fact the person he or she claims to be. It is therefore necessary that the European Digital Identity Wallets rely on the legal identity of citizens, other residents or legal entities. Trust in the European Digital Identity Wallets would be enhanced by the fact that issuing parties are required to implement appropriate technical and organisational measures to ensure a level of security commensurate to the risks raised for the rights and freedoms of the natural persons, in line with Regulation (EU) 2016/679.

(10) In order to achieve a high level of security and trustworthiness, this Regulation establishes the requirements for European Digital Identity Wallets. The conformity of European Digital Identity Wallets with those requirements should be certified by accredited public or private sector bodies designated by Member States. Relying on a certification scheme based on the availability of commonly agreed standards with Member States should ensure a high level of trust and interoperability. Certification should in particular rely on the relevant European cybersecurity certifications schemes established pursuant to Regulation (EU) 2019/881[20]. Such certification should be without prejudice to certification as regards personal data processing pursuant to Regulation (EC) 2016/679

(11) European Digital Identity Wallets should ensure the highest level of security for the personal data used for authentication irrespective of whether such data is stored locally or on cloud-based solutions, taking into account the different levels of risk. Using biometrics to authenticate is one of the identifications methods providing a high level of confidence, in particular when used in combination with other elements of authentication. Since biometrics represents a unique characteristic of a person, the use of biometrics requires organisational and security measures, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons and in accordance with Regulation 2016/679.

(12) To ensure that the European Digital Identity framework is open to innovation, technological development and future-proof, Member States should be encouraged to set-up jointly sandboxes to test innovative solutions in a controlled and secure environment in particular to improve the functionality, protection of personal data, security and interoperability of the solutions and to inform future updates of technical references and legal requirements. This environment should foster the inclusion of European Small and Medium Enterprises, start-ups and individual innovators and researchers.

---

[20] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15

www.parlament.gv.at

(13) Regulation (EU) No 2019/1157[21] strengthens the security of identity cards with enhanced security features by August 2021. Member States should consider the feasibility of notifying them under electronic identification schemes to extend the cross-border availability of electronic identification means.

(14) The process of notification of electronic identification schemes should be simplified and accelerated to promote the access to convenient, trusted, secure and innovative authentication and identification solutions and, where relevant, to encourage private identity providers to offer electronic identification schemes to Member State's authorities for notification as national electronic identity card schemes under Regulation 910/2014.

(15) Streamlining of the current notification and peer-review procedures will prevent heterogeneous approaches to the assessment of various notified electronic identification schemes and facilitate trust-building between Member States. New, simplified, mechanisms should foster Member States' cooperation on the security and interoperability of their notified electronic identification schemes.

(16) Member States should benefit from new, flexible tools to ensure compliance with the requirements of this Regulation and of the relevant implementing acts. This Regulation should allow Member States to use reports and assessments performed by accredited conformity assessment bodies or voluntary ICT security certification schemes, such as certification schemes to be established at Union level under Regulation (EU) 2019/881, to support their claims on the alignment of the schemes or of parts thereof with the requirements of the Regulation on the interoperability and the security of the notified electronic identification schemes.

(17) Service providers use the identity data provided by the set of person identification data available from electronic identification schemes pursuant to Regulation (EU) No 910/2014 in order to match users from another Member State with the legal identity of that user. However, despite the use of the eIDAS data set, in many cases ensuring an accurate match requires additional information about the user and specific unique identification procedures at national level. To further support the usability of electronic identification means, this Regulation should require Member States to take specific measures to ensure a correct identity match in the process of electronic identification. For the same purpose, this Regulation should also extend the mandatory minimum data set and require the use of a unique and persistent electronic identifier in conformity with Union law in those cases where it is necessary to legally identify the user upon his/her request in a unique and persistent way.

(18) In line with Directive (EU) 2019/882[22], persons with disabilities should be able to use the European digital identity wallets, trust services and end-user products used in the provision of those services on an equal basis with other users.

(19) This Regulation should not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid

[21] 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).

[22] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

www.parlament.gv.at

down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.

(20) The provision and use of trust services are becoming increasingly important for international trade and cooperation. International partners of the EU are establishing trust frameworks inspired by Regulation (EU) No 910/2014. Therefore, in order to facilitate the recognition of such services and their providers, implementing legislation may set the conditions under which trust frameworks of third countries could be considered equivalent to the trust framework for qualified trust services and providers in this Regulation, as a complement to the possibility of the mutual recognition of trust services and providers established in the Union and in third countries in accordance with Article 218 of the Treaty.

(21) This Regulation should build on Union acts ensuring contestable and fair markets in the digital sector. In particular, it builds on the Regulation XXX/XXXX [Digital Markets Act], which introduces rules for providers of core platform services designated as gatekeepers and, among others, prohibits gatekeepers to require business users to use, offer or interoperate with an identification service of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper. Article 6(1)(f) of the Regulation XXX/XXXX [Digital Markets Act] requires gatekeepers to allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services. According to Article 2 (15) of [Digital Markets Act] identification services constitute a type of ancillary services. Business users and providers of ancillary services should therefore be able to access such hardware or software features, such as secure elements in smartphones, and to interoperate with them through the European Digital Identity Wallets or Member States' notified electronic identification means.

(22) In order to streamline the cybersecurity obligations imposed on trust service providers, as well as to enable these providers and their respective competent authorities to benefit from the legal framework established by Directive XXXX/XXXX (NIS2 Directive), trust services are required to take appropriate technical and organisational measures pursuant to Directive XXXX/XXXX (NIS2 Directive), such as measures addressing system failures, human error, malicious actions or natural phenomena in order to manage the risks posed to the security of network and information systems which those providers use in the provision of their services as well as to notify significant incidents and cyber threats in accordance with Directive XXXX/XXXX (NIS2 Directive). With regard to the reporting of incidents, trust service providers should notify any incidents having a significant impact on the provision of their services, including such caused by theft or loss of devices, network cable damages or incidents occurred in the context of identification of persons. The cybersecurity risk management requirements and reporting obligations under Directive XXXXXX [NIS2] should be considered complementary to the requirements imposed on trust service providers under this Regulation. Where appropriate, established national practices or guidance in relation to the implementation of security and reporting requirements and supervision of compliance with such requirements under Regulation (EU) No 910/2014 should continue to be applied by the competent authorities designated under Directive XXXX/XXXX (NIS2 Directive). Any requirements pursuant to this Regulation do not affect the obligation to notify personal data breaches under Regulation (EU) 2016/679.

www.parlament.gv.at

(23) Due consideration should be given to ensure effective cooperation between the NIS and eIDAS authorities. In cases where the supervisory body under this Regulation is different from the competent authorities designated under Directive XXXX/XXXX [NIS2], those authorities should cooperate closely, in a timely manner by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in this Regulation and Directive XXXX/XXXX [NIS2]. In particular, the supervisory bodies under this Regulation should be entitled to request the competent authority under Directive XXXXX/XXXX [NIS2] to provide the relevant information needed to grant the qualified status and to carry out supervisory actions to verify compliance of the trust service providers with the relevant requirements under NIS 2 or require them to remedy non-compliance.

(24) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new pan-European electronic registered delivery services and ensure that the identification of the recipients is ensured with a higher level of confidence than the identification of the sender.

(25) In most cases, citizens and other residents cannot digitally exchange, across borders, information related to their identity, such as addresses, age and professional qualifications, driving licenses and other permits and payment data, securely and with a high level of data protection.

(26) It should be possible to issue and handle trustworthy digital attributes and contribute to reducing administrative burden, empowering citizens and other residents to use them in their private and public transactions. Citizens and other residents should be able, for instance, to demonstrate ownership of a valid driving license issued by an authority in one Member State, which can be verified and relied upon by the relevant authorities in other Member States, to rely on their social security credentials or on future digital travel documents in a cross border context.

(27) Any entity that collects, creates and issues attested attributes such as diplomas, licences, certificates of birth should be able to become a provider of electronic attestation of attributes. Relying parties should use the electronic attestations of attributes as equivalent to attestations in paper format. Therefore, an electronic attestation of attributes should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic attestation of attributes. To that effect, general requirements should be laid down to ensure that a qualified electronic attestation of attributes has the equivalent legal effect of lawfully issued attestations in paper form. However, those requirements should apply without prejudice to Union or national law defining additional sector specific requirements as regards form with underlying legal effects and, in particular, the cross-border recognition of qualified electronic attestation of attributes, where appropriate.

(28) Wide availability and usability of the European Digital Identity Wallets require their acceptance by private service providers. Private relying parties providing services in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the use of European Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by national or Union law or by contractual obligation. Where very large online platforms as defined in Article 25.1. of Regulation [reference DSA Regulation] require users to

www.parlament.gv.at

authenticate to access online services, those platforms should be mandated to accept the use of European Digital Identity Wallets upon voluntary request of the user. Users should be under no obligation to use the wallet to access private services, but if they wish to do so, large online platforms should accept the European Digital Identity Wallet for this purpose while respecting the principle of data minimisation. Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service and economic transactions this is necessary to increase the protection of users from fraud and secure a high level of data protection. Self-regulatory codes of conduct at Union level ('codes of conduct') should be developed in order to contribute to wide availability and usability of electronic identification means including European Digital Identity Wallets within the scope of this Regulation. The codes of conduct should facilitate wide acceptance of electronic identification means including European Digital Identity Wallets by those service providers which do not qualify as very large platforms and which rely on third party electronic identification services for user authentication. They should be developed within 12 months of the adoption of this Regulation. The Commission should assess the effectiveness of these provisions for the availability and usability for the user of the European Digital Identity Wallets after 18 months of their deployment and revise the provisions to ensure their acceptance by means of delegated acts in the light of this assessment.

(29) The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. This feature should become a basic design feature thereby reinforcing convenience and personal data protection including minimisation of processing of personal data.

(30) Attributes provided by the qualified trust service providers as part of the qualified attestation of attributes should be verified against the authentic sources either directly by the qualified trust service provider or via designated intermediaries recognised at national level in accordance with national or Union law for the purpose of secure exchange of attested attributes between identity or attestation of attributes' service providers and relying parties.

(31) Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to allow identification of customers and the exchange of specific attributes necessary to comply with, for example, customer due diligence requirements under the Anti Money Laundering Regulation, [reference to be added after the adoption of the proposal], with suitability requirements stemming from investor protection legislation, or to support the fulfilment of strong customer authentication requirements for account login and initiation of transactions in the field of payment services.

(32) Website authentication services provide users with assurance that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The use of website authentication services by websites is voluntary. However, in order for website authentication to become a means to increasing trust, providing a better experience for the user and furthering growth in the internal market, this Regulation lays down minimal security and liability obligations for the providers of website authentication services and their services. To that end, web-browsers should ensure support and interoperability with Qualified certificates for website authentication pursuant to Regulation (EU) No 910/2014. They should recognise and display Qualified certificates for website

www.parlament.gv.at

authentication to provide a high level of assurance, allowing website owners to assert their identity as owners of a website and users to identify the website owners with a high degree of certainty. To further promote their usage, public authorities in Member States should consider incorporating Qualified certificates for website authentication in their websites.

(33) Many Member States have introduced national requirements for services providing secure and trustworthy digital archiving in order to allow for the long term preservation of electronic documents and associated trust services. To ensure legal certainty and trust, it is essential to provide a legal framework to facilitate the cross border recognition of qualified electronic archiving services. That framework could also open new market opportunities for Union trust service providers.

(34) Qualified electronic ledgers record data in a manner that ensures the uniqueness, authenticity and correct sequencing of data entries in a tamper proof manner. An electronic ledger combines the effect of time stamping of data with certainty about the data originator similar to e-signing and has the additional benefit of enabling more decentralised governance models that are suitable for multi-party co-operations. For example, it creates a reliable audit trail for the provenance of commodities in cross-border trade, supports the protection of intellectual property rights, enables flexibility markets in electricity, provides the basis for advanced solutions for self-sovereign identity and supports more efficient and transformative public services. To prevent fragmentation of the internal market, it is important to define a pan-European legal framework that allows for the cross-border recognition of trust services for the recording of data in electronic ledgers.

(35) The certification as qualified trust service providers should provide legal certainty for use cases that build on electronic ledgers. This trust service for electronic ledgers and qualified electronic ledgers and the certification as qualified trust service provider for electronic ledgers should be notwithstanding the need for use cases to comply with Union law or national law in compliance with Union law. Use cases that involve the processing of personal data must comply with Regulation (EU) 2016/679. Use cases that involve crypto assets should be compatible with all applicable financial rules for example with the Markets in Financial Instruments Directive[23], the Payment Services Directive[24] and the future Markets in Crypto Assets Regulation[25].

(36) In order to avoid fragmentation and barriers, due to diverging standards and technical restrictions, and to ensure a coordinated process to avoid endangering the implementation of the future European Digital Identity framework, a process for close and structured cooperation between the Commission, Member States and the private sector is needed. To achieve this objective, Member States should cooperate within the framework set out in the Commission Recommendation XXX/XXXX [Toolbox for a

---

[23] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance, *OJ L 173, 12.6.2014, p. 349–496.*

[24] 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, *OJ L 337, 23.12.2015, p. 35–127.*

[25] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final.

www.parlament.gv.at

coordinated approach towards a European Digital Identity Framework][26] to identify a Toolbox for a European Digital Identity framework. The Toolbox should include a comprehensive technical architecture and reference framework, a set of common standards and technical references and a set of guidelines and descriptions of best practices covering at least all aspects of the functionalities and interoperability of the European Digital Identity Wallets including eSignatures and of the qualified trust service for attestation of attributes as laid out in this regulation. In this context, Member States should also reach agreement on common elements of a business model and fee structure of the European Digital Identity Wallets, to facilitate take up, in particular by small and medium sized companies in a cross-border context. The content of the toolbox should evolve in parallel with and reflect the outcome of the discussion and process of adoption of the European Digital Identity Framework.

(37) The European Data Protection Supervisor has been consulted pursuant to Article 42 (1) of Regulation (EU) 2018/1525 of the European Parliament and of the Council[27].

(38) Regulation (EU) 910/2014 should therefore be amended accordingly,

HAVE ADOPTED THIS REGULATION:

Article 1

Regulation (EU) 910/2014 is amended as follows:

(1) Article 1 is replaced by the following:

'This Regulations aims at ensuring the proper functioning of the internal market and providing an adequate level of security of electronic identification means and trust services. For these purposes, this Regulation:

(a) lays down the conditions under which Member States shall provide and recognise electronic identification means of natural and legal persons, falling under a notified electronic identification scheme of another Member State;

(b) lays down rules for trust services, in particular for electronic transactions;

(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic archiving and electronic attestation of attributes, the management of remote electronic signature and seal creation devices, and electronic ledgers;

(d) lays down the conditions for the issuing of European Digital Identity Wallets by Member States.';

(2) Article 2 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. This Regulation applies to electronic identification schemes that have been notified by a Member State, European Digital Identity Wallets

[26] [insert reference once adopted]

[27] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

www.parlament.gv.at

issued by Member States and to trust service providers that are established in the Union.';

(b) paragraph 3 is replaced by the following:

'3. This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to sector specific requirements as regards form with underlying legal effects.';

(3) Article 3 is amended as follows:

(a) point (2) is replaced by the following:

'(2) 'electronic identification means' means a material and/or immaterial unit, including European Digital Identity Wallets or ID cards following Regulation 2019/1157, containing person identification data and which is used for authentication for an online or offline service;';

(b) point (4) is replaced by the following:

'(4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means, are issued to natural or legal persons or natural persons representing legal persons;';

(c) point (14) is replaced by the following:

'(14) 'certificate for electronic signature' means an electronic attestation or set of attestations which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;';

(d) point (16) is replaced by the following:

'(16) 'trust service' means an electronic service normally provided against payment which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, electronic attestation of attributes and certificates related to those services;

(b) the creation, verification and validation of certificates for website authentication;

(c) the preservation of electronic signatures, seals or certificates related to those services;

(d) the electronic archiving of electronic documents;

(e) the management of remote electronic signature and seal creation devices;

(f) the recording of electronic data into an electronic ledger.';

(e) point (21) is replaced by the following:

'(21) 'product' means hardware or software, or relevant components of hardware and / or software, which are intended to be used for the provision of electronic identification and trust services;';

(f) the following points (23a) and (23b) are inserted:

www.parlament.gv.at

‘(23a) ‘remote qualified signature creation device’ means a qualified electronic signature creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a signatory;

(23b) ‘remote qualified seal creation device’ means a qualified electronic seal creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a seal creator;’;

(g) point (29) is replaced by the following:

‘(29) ‘certificate for electronic seal’ means an electronic attestation or set of attestations that links electronic seal validation data to a legal person and confirms the name of that person;’;

(h) point (41) is replaced by the following:

‘(41) ‘validation’ means the process of verifying and confirming that an electronic signature or a seal or person identification data or an electronic attestation of attributes is valid;’

(i) the following points (42) to (55) are added:

‘(42) ‘European Digital Identity Wallet’ is a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals;

(43) ‘attribute’ is a feature, characteristic or quality of a natural or legal person or of an entity, in electronic form;

(44) ‘electronic attestation of attributes’ means an attestation in electronic form that allows the authentication of attributes;

(45) ‘qualified electronic attestation of attributes’ means an electronic attestation of attributes, which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;

(46) ‘authentic source’ is a repository or system, held under the responsibility of a public sector body or private entity, that contains attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in national law;

(47) ‘electronic archiving’ means a service ensuring the receipt, storage, deletion and transmission of electronic data or documents in order to guarantee their integrity, the accuracy of their origin and legal features throughout the conservation period;

(48) ‘qualified electronic archiving service’ means a service that meets the requirements laid down in Article 45g;

(49) ‘EU Digital Identity Wallet Trust Mark’ means an indication in a simple, recognisable and clear manner that a Digital Identity Wallet has been issued in accordance with this Regulation;

www.parlament.gv.at

(50) ‘strong user authentication’ means an authentication based on the use of two or more elements categorised as user knowledge , possession and inherence that are independent, in such a way that the breach of one does not compromise the reliability of the others, and is designed in such a way to protect the confidentiality of the authentication data;

(51) ‘user account’ means a mechanism that allows a user to access public or private services on the terms and conditions established by the service provider;

(52) ‘credential’ means a proof of a person’s abilities, experience, right or permission;

(53) ‘electronic ledger’ means a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering’;

(54) ‘Personal data’ means any information as defined in point 1 of Article 4 of Regulation (EU) 2016/679.’;

(55) ‘unique identification’ means a process where person identification data or person identification means are matched with or linked to an existing account belonging to the same person.’;

(4) Article 5 is replaced by the following:

‘*Article 5*

Pseudonyms in electronic transaction

Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.’;

(5) in Chapter II the heading is replaced by the following:

‘SECTION I

ELECTRONIC IDENTIFICATION’;

(6) Article 6 is deleted;

(7) the following Articles (6a, 6b, 6c and 6d) are inserted:

‘*Article 6a*

European Digital Identity Wallets

1. For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless access to cross-border public and private services, each Member State shall issue a European Digital Identity Wallet within 12 months after the entry into force of this Regulation.

2. European Digital Identity Wallets shall be issued:

   (a) by a Member State;

   (b) under a mandate from a Member State;

   (c) independently but recognised by a Member State.

3. European Digital Identity Wallets shall enable the user to:

   (a) securely request and obtain, store, select, combine and share, in a manner that is transparent to and traceable by the user, the necessary legal person

www.parlament.gv.at

identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services;

(b) sign by means of qualified electronic signatures.

4. Digital Identity Wallets shall, in particular:

(a) provide a common interface:

(1) to qualified and non-qualified trust service providers issuing qualified and non-qualified electronic attestations of attributes or other qualified and non-qualified certificates for the purpose of issuing such attestations and certificates to the European Digital Identity Wallet;

(2) for relying parties to request and validate person identification data and electronic attestations of attributes;

(3) for the presentation to relying parties of person identification data, electronic attestation of attributes or other data such as credentials, in local mode not requiring internet access for the wallet;

(4) for the user to allow interaction with the European Digital Identity Wallet and display an "EU Digital Identity Wallet Trust Mark";

(b) ensure that trust service providers of qualified attestations of attributes cannot receive any information about the use of these attributes;

(c) meet the requirements set out in Article 8 with regards to assurance level "high", in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication;

(d) provide a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestations of attributes;

(e) ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represent the natural or legal person is associated with it.

5. Member States shall provide validation mechanisms for the European Digital Identity Wallets:

(a) to ensure that its authenticity and validity can be verified;

(b) to allow relying parties to verify that the attestations of attributes are valid;

(c) to allow relying parties and qualified trust service providers to verify the authenticity and validity of attributed person identification data.

6. The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'. The use of the European Digital Identity Wallets shall be free of charge to natural persons.

7. The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity

www.parlament.gv.at

Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held. If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.

8. Article 11 shall apply mutatis mutandis to the European Digital Identity Wallet.

9. Article 24(2), points (b), (e), (g), and (h) shall apply mutatis mutandis to Member States issuing the European Digital Identity Wallets.

10. The European Digital Identity Wallet shall be made accessible for persons with disabilities in accordance with the accessibility requirements of Annex I to Directive 2019/882.

11. Within 6 months of the entering into force of this Regulation, the Commission shall establish technical and operational specifications and reference standards for the requirements referred to in paragraphs 3, 4 and 5 by means of an implementing act on the implementation of the European Digital Identity Wallet. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 6b

European Digital Identity Wallets Relying Parties

1. Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall communicate it to the Member State where the relying party is established to ensure compliance with requirements set out in Union law or national law for the provision of specific services. When communicating their intention to rely on European Digital Identity wallets, they shall also inform about the intended use of the European Digital Identity Wallet.

2. Member States shall implement a common mechanism for the authentication of relying parties

3. Relying parties shall be responsible for carrying out the procedure for authenticating person identification data and electronic attestation of attributes originating from European Digital Identity Wallets.

4. Within 6 months of the entering into force of this Regulation, the Commission shall establish technical and operational specifications for the requirements referred to in paragraphs 1 and 2 by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).

Article 6c

Certification of the European Digital Identity Wallets

1. European Digital Identity Wallets that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a

www.parlament.gv.at

paragraphs 3, 4 and 5 in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

2. Compliance with the requirements set out in paragraphs 3, 4 and 5 of Article 6a related to the personal data processing operations carried out by the issuer of the European Digital Identity Wallets shall be certified pursuant to Regulation (EU) 2016/679.

3. The conformity of European Digital Identity Wallets with the requirements laid down in article 6a paragraphs 3, 4 and 5 shall be certified by accredited public or private bodies designated by Member States.

4. Within 6 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish a list of standards for the certification of the European Digital Identity Wallets referred to in paragraph 3.

5. Member States shall communicate to the Commission the names and addresses of the public or private bodies referred to in paragraph 3. The Commission shall make that information available to Member States.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 3.

Article 6d

Publication of a list of certified European Digital Identity Wallets

1. Member States shall inform the Commission without undue delay of the European Digital Identity Wallets that have been issued pursuant to Article 6a and certified by the bodies referred to in Article 6c paragraph 3 They shall also inform the Commission, without undue delay where the certification is cancelled.

2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified European Digital Identity Wallets.

3. Within 6 months of the entering into force of this Regulation, the Commission shall define formats and procedures applicable for the purposes of paragraph 1. by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).

(8) the following heading is inserted before Article 7:

‘SECTION II

ELECTRONIC IDENTIFICATION SCHEMES’;

(9) the introductory sentence of Article 7 is replaced by the following:

‘Pursuant to Article 9(1) Member States shall notify, within 12 months after the entry into force of this Regulation at least one electronic identification scheme including at least one identification means:’;

(10) in Article 9 paragraphs 2 and 3 are replaced by the following:

‘2. The Commission shall publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.

www.parlament.gv.at

3. The Commission shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within one month from the date of receipt of that notification.';

(11) the following Article 10a is inserted:

'*Article 10a*

Security breach of the European Digital Identity Wallets

1. Where European Digital Wallets issued pursuant to Article 6a and the validation mechanisms referred to in Article 6a(5) points (a), (b) and (c) are breached or partly compromised in a manner that affects their reliability or the reliability of the other European Digital Identity Wallets, the issuing Member State shall, without delay, suspend the issuance and revoke the validity of the European Digital Identity Wallet and inform the other Member States and the Commission accordingly.

2. Where the breach or compromise referred to in paragraph 1 is remedied, the issuing Member State shall re-establish the issuance and the use of the European Digital Identity Wallet and inform other Member States and the Commission without undue delay.

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the Member State concerned shall withdraw the European Digital Wallet concerned and inform the other Member States and the Commission on the withdrawal accordingly. Where it is justified by the severity of the breach, the European Digital Identity Wallet concerned shall be withdrawn without delay.

4. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 6d without undue delay.

5. Within 6 months of the entering into force of this Regulation, the Commission shall further specify the measures referred to in paragraphs 1 and 3 by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).

(12) the following Article 11a is inserted:

'*Article 11a*

Unique Identification

1. When notified electronic identification means and the European Digital Identity Wallets are used for authentication, Member States shall ensure unique identification.

2. Member States shall, for the purposes of this Regulation, include in the minimum set of person identification data referred to in Article 12.4.(d), a unique and persistent identifier in conformity with Union law, to identify the user upon their request in those cases where identification of the user is required by law.

3. Within 6 months of the entering into force of this Regulation, the Commission shall further specify the measures referred to in paragraph 1 and 2 by means of

www.parlament.gv.at

an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).

(13) Article 12 is amended as follows:

(a) in paragraph 3, points (c) and (d) are deleted;

(b) in paragraph 4, point (d) is replaced by the following:

‘(d) a reference to a minimum set of person identification data necessary to uniquely and persistently represent a natural or legal person;’;

(c) in paragraph 6, point (a) of is replaced by the following:

‘(a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability, unique identification and assurance levels;’;

(14) the following Article 12a is inserted:

‘*Article 12a*

Certification of electronic identification schemes

1. Conformity of notified electronic identification schemes with the requirements laid down in Article 6a, Article 8 and Article 10 may be certified by public or private bodies designated by Member States.

2. The peer-review of electronic identification schemes referred to in Article 12(6), point (c) shall not apply to electronic identification schemes or part of such schemes certified in accordance with paragraph 1. Member States may use a certificate or a Union statement of conformity issued in accordance with a relevant European cybersecurity certification scheme established pursuant to Regulation (EU) 2019/881 to demonstrate compliance of such schemes with the requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes.

3. Member States shall notify to the Commission with the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.’;

(15) the following heading is inserted after Article 12a:

‘SECTION III

CROSS-BORDER RELIANCE ON ELECTRONIC IDENTIFICATION MEANS’;

(16) the following Articles 12b and 12c are inserted:

‘Article 12b

Cross-border reliance on European Digital Identity Wallets

1. Where Member States require an electronic identification using an electronic identification means and authentication under national law or by administrative practice to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets issued in compliance with this Regulation.

www.parlament.gv.at

2. Where private relying parties providing services are required by national or Union law, to use strong user authentication for online identification, or where strong user authentication is required by contractual obligation, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a.

3. Where very large online platforms as defined in Regulation [reference DSA Regulation] Article 25.1. require users to authenticate to access online services, they shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a strictly upon voluntary request of the user and in respect of the minimum attributes necessary for the specific online service for which authentication is requested, such as proof of age.

4. The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to wide availability and usability of European Digital Identity Wallets within the scope of this Regulation. These codes of conduct shall ensure acceptance of electronic identification means including European Digital Identity Wallets within the scope of this Regulation in particular by service providers relying on third party electronic identification services for user authentication. The Commission will facilitate the development of such codes of conduct in close cooperation with all relevant stakeholders and encourage service providers to complete the development of codes of conduct within 12 months of the adoption of this Regulation and effectively implement them within 18 months of the adoption of the Regulation.

5. The Commission shall make an assessment within 18 months after deployment of the European Digital Identity Wallets whether on the basis of evidence showing availability and usability of the European Digital Identity Wallet, additional private online service providers shall be mandated to accept the use of the European Digital identity Wallet strictly upon voluntary request of the user. Criteria of assessment may include extent of user base, cross-border presence of service providers, technological development, evolution in usage patterns. The Commission shall be empowered to adopt delegated acts based on this assessment, regarding a revision of the requirements for recognition of the European Digital Identity wallet under points 1 to 4 of this article.

6. For the purposes of this Article, European Digital Identity Wallets shall not be subject to the requirements referred to in articles 7 and 9.

Article 12c

Mutual recognition of other electronic identification means

1. Where electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access an online service provided by a public sector body in a Member State, the electronic identification means, issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that online service, provided that the following conditions are met:

www.parlament.gv.at

(a) the electronic identification means is issued under an electronic identification scheme that is included in the list referred to in Article 9;

(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that online service in the Member State concerned, and in any case not lower than an assurance level 'substantial';

(c) the relevant public sector body in the Member State concerned uses the assurance level 'substantial' or 'high' in relation to accessing that online service.

Such recognition shall take place no later than 6 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued within the scope of an electronic identification scheme included in the list referred to in Article 9 and which corresponds to the assurance level 'low' may be recognised by public sector bodies for the purposes of cross-border authentication for the online service provided by those bodies.';

(17) In Article 13, paragraph 1 is replaced by the following:

'1. Notwithstanding paragraph 2 of this Article, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation and with the cybersecurity risk management obligations under Article 18 of the Directive XXXX/XXXX [NIS2].';

(18) Article 14 is replaced by the following:

'*Article 14*

International aspects

1. The Commission may adopt implementing acts, in accordance with Article 48(2), setting out the conditions under which the requirements of a third country applicable to the trust service providers established in its territory and to the trust services they provide can be considered equivalent to the requirements applicable to qualified trust service providers established in the Union and to the qualified trust services they provide.

2. Where the Commission has adopted an implementing act pursuant to paragraph 1 or concluded an international agreement on the mutual recognition of trust services in accordance with Article 218 of the Treaty, trust services provided by providers established in the third country concerned shall be considered equivalent to qualified trust services provided by qualified trust service providers established in the Union.';

(19) Article 15 is replaced by the following:

'*Article 15*

Accessibility for persons with disabilities

The provision of Trust services and end-user products used in the provision of those services shall be made accessible for persons with disabilities in accordance with the

www.parlament.gv.at

accessibility requirements of Annex I of Directive 2019/882 on the accessibility requirements for products and services.';

(20) Article 17 is amended as follows:

(a) paragraph 4 is amended as follows:

(1) point (c) of paragraph 4 is replaced by the following:

'(c) to inform the relevant national competent authorities of the Member States concerned, designated pursuant to Directive (EU) XXXX/XXXX [NIS2], of any significant breaches of security or loss of integrity they become aware of in the performance of their tasks. where the significant breach of security or loss of integrity concerns other Member States, the supervisory body shall inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX (NIS2);';

(2) point (f) is replaced by the following:

'(f) to cooperate with supervisory authorities established under Regulation (EU) 2016/679, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules have been breached and about security breaches which constitute personal data breaches;';

(b) paragraph 6 is replaced by the following:

'6. By 31 March each year, each supervisory body shall submit to the Commission a report on its main activities during the previous calendar year.';

(c) paragraph 8 is replaced by the following:

'8. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, further specify the tasks of the Supervisory Authorities referred to in paragraph 4 and define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(21) Article 18 is amended as follows:

(a) the title of Article 18 is replaced by the following:

'**Mutual assistance and cooperation**';

(b) paragraph 1 is replaced by the following:

'1. Supervisory bodies shall cooperate with a view to exchanging good practice and information regarding the provision of trust services.';

(c) the following paragraphs 4 and 5 are added:

'4. Supervisory bodies and national competent authorities under Directive (EU) XXXX/XXXX of the European Parliament and of the Council [NIS2] shall cooperate and assist each other to ensure that trust service providers comply with the requirements laid down in this Regulation

www.parlament.gv.at

and in Directive (EU) XXXX/XXXX [NIS2]. The supervisory body shall request the national competent authority under Directive XXXX/XXXX [NIS2] to carry out supervisory actions to verify compliance of the trust service providers with the requirements under Directive XXXX/XXXX (NIS2), to require the trust service providers to remedy any failure to comply with those requirements, to provide timely the results of any supervisory activities linked to trust service providers and to inform the supervisory bodies about relevant incidents notified in accordance with Directive XXXX/XXXX [NIS2].

5. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Supervisory Authorities referred to in paragraph 1.';

(22) Article 20 is amended as follows:

(a) paragraph 1 is replaced by the following

'1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. the audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 18 of Directive (EU) XXXX/XXXX [NIS2]. qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.';

(b) in paragraph 2, the last sentence is replaced by the following

'Where personal data protection rules appear to have been breached, the supervisory body shall inform the supervisory authorities under Regulation (EU) 2016/679 of the results of its audits.';

(c) paragraphs 3 and 4 are replaced by the following:

'3. Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable.

where that provider does not provide a remedy and, where applicable within the time limit set by the supervisory body, the supervisory body, taking into account in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the service concerned which it provides and, request it, where applicable within a set time limit, to comply with the requirements of Directive XXXX/XXXX[NIS2]. The supervisory body shall inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1).

The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

4. Within 12 months of the entering into force of this regulation, the Commission shall, by means of implementing acts, establish reference number for the following standards:

www.parlament.gv.at

(a) the accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;

(b) the auditing requirements for the conformity assessment bodies to carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1, carried out by the conformity assessment bodies;

(c) the conformity assessment schemes for carrying out the conformity assessment of the qualified trust service providers by the conformity assessment bodies and for the provision of the conformity assessment report referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(23) Article 21 is amended as follows:

(a) paragraph 2 is replaced by the following:

'2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

In order to verify the compliance of the trust service provider with the requirements laid down in Article 18 of Dir XXXX [NIS2], the supervisory body shall request the competent authorities referred to in Dir XXXX [NIS2] to carry out supervisory actions in that regard and to provide information about the outcome within three days from their completion.

Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

Where the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.';

(b) paragraph 4 is replaced with the following:

'4. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, define the formats and procedures of the notification and verification for the purposes of paragraphs 1 and 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(24) in Article 23 the following paragraph 2a is added:

www.parlament.gv.at

‘2a. Paragraph 1 and 2 shall also apply to trust service providers established in third countries and to the services they provide, provided that they have been recognised in the Union in accordance with Article 14.’;

(25) Article 24 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. When issuing a qualified certificate or a qualified electronic attestation of attributes for a trust service, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider, either directly or by relying on a third party, in any of the following ways:

(a) by means of a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance levels ‘substantial’ or ‘high’;

(b) by means of qualified electronic attestations of attributes or a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a), (c) or (d);

(c) by using other identification methods which ensure the identification of the natural person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;

(d) through the physical presence of the natural person or of an authorised representative of the legal person by appropriate procedures and in accordance with national laws if other means are not available.’;

(b) the following paragraph 1a is inserted:

‘1a. Within 12 months after the entry into force of this Regulation, the Commission shall by means of implementing acts, set out minimum technical specifications, standards and procedures with respect to the verification of identity and attributes in accordance with paragraph 1, point c. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(c) paragraph 2 is amended as follows:

(1) point (d) is replaced by the following:

‘(d) before entering into a contractual relationship, inform, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;’;

(2) the new points (fa) and (fb) are inserted:

www.parlament.gv.at

‘(fa) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the qualified trust service. Notwithstanding the provisions of Article 18 of Directive EU XXXX/XXX [NIS2], those measures shall include at least the following:

(i) measures related to registration and on-boarding procedures to a service;

(ii) measures related to procedural or administrative checks;

(iii) measures related to the management and implementation of services.

(fb) notify the supervisory body and, where applicable, other relevant bodies of any linked breaches or disruptions in the implementation of the measures referred to in paragraph (fa), points (i), (ii) and, (iii) that has a significant impact on the trust service provided or on the personal data maintained therein.’;

(3) point (g) and (h) are replaced by the following:

‘(g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible;

(h) record and keep accessible for as long as necessary after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;’;

(4) point (j) is deleted;

(d) the following paragraph 4a is inserted:

‘4a. Paragraph 3 and 4 shall apply accordingly to the revocation of electronic attestations of attributes.’;

(e) paragraph 5 is replaced by the following:

‘5. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the requirements referred to in paragraph 2. compliance with the requirements laid down in this Article shall be presumed, where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(f) the following paragraph 6 is inserted:

‘6. The Commission shall be empowered to adopt delegated acts regarding the additional measures referred to in paragraph 2(fa).’;

(26) In Article 28, paragraph 6 is replaced by the following:

www.parlament.gv.at

‘6. Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(27) In Article 29, the following new paragraph 1a is added:

‘1a. Generating, managing and duplicating electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider providing a qualified trust service for the management of a remote electronic qualified signature creation device.’;

(28) the following Article 29a is inserted:

‘*Article 29a*

Requirements for a qualified service for the management of remote electronic signature creation devices

1. The management of remote qualified electronic signature creation devices as a qualified service may only be carried out by a qualified trust service provider that:

(a) Generates or manages electronic signature creation data on behalf of the signatory;

(b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data only for back-up purposes provided the following requirements are met:

the security of the duplicated datasets must be at the same level as for the original datasets;

the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

(c) complies with any requirements identified in the certification report of the specific remote qualified signature creation device issued pursuant to Article 30.

2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for the purposes of paragraph 1.’;

(29) In Article 30, the following paragraph 3a is inserted:

‘3a. The certification referred to in paragraph 1 shall be valid for 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be withdrawn.’;

(30) In Article 31, paragraph 3 is replaced by the following:

‘3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts

www.parlament.gv.at

shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(31) Article 32 is amended as follows:

(a) in paragraph 1, the following sub-paragraph is added:

'Compliance with the requirements laid down in the first sub-paragraph shall be presumed where the validation of qualified electronic signatures meet the standards referred to in paragraph 3.';

(b) paragraph 3 is replaced by the following:

'3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(32) Article 34 is replaced by the following:

'*Article 34*

Qualified preservation service for qualified electronic signatures

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

2. Compliance with the requirements laid down in the paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet the standards referred to in paragraph 3.

3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to In Article 48(2).';

(33) Article 37 is amended as follows:

(a) the following paragraph 2a is inserted:

'2a. Compliance with the requirements for advanced electronic seals referred to in Article 36 and in paragraph 5 of this Article shall be presumed where an advanced electronic seal meets the standards referred to in paragraph 4.';

(b) paragraph 4 is replaced by the following:

'4. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(34) Article 38 is amended as follows:

(a) paragraph 1 is replaced by the following:

www.parlament.gv.at

‘1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets the standards referred to in paragraph 6.’;

(b) paragraph 6 is replaced by the following:

‘6. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(35) the following Article 39a is inserted:

‘*Article 39a*

Requirements for a qualified service for the management of remote electronic seal creation devices

Article 29a shall apply mutatis mutandis to a qualified service for the management of remote electronic seal creation devices.’;

(36) Article 42 is amended as follows:

(a) the following new paragraph 1a is inserted:

‘1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meet the standards referred to in paragraph 2.’;

(b) paragraph 2 is replaced by the following

‘2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(37) Article 44 is amended as follows:

(a) the following paragraph 1a is inserted:

‘1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets the standards referred to in paragraph 2.’;

(b) paragraph 2 is replaced by the following:

‘2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(38) Article 45 is replaced by the following:

‘*Article 45*

Requirements for qualified certificates for website authentication

www.parlament.gv.at

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. Qualified certificates for website authentication shall be deemed compliant with the requirements laid down in Annex IV where they meet the standards referred to in paragraph 3.

2. Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. For those purposes web-browsers shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1, with the exception of enterprises, considered to be microenterprises and small enterprises in accordance with Commission Recommendation 2003/361/EC in the first 5 years of operating as providers of web-browsing services.

3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide the specifications and reference numbers of standards for qualified certificates for website authentication referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(39) the following sections 9, 10 and 11 are inserted after Article 45:

'SECTION 9

ELECTRONIC ATTESTATION OF ATTRIBUTES

Article 45a

Legal effects of electronic attestation of attributes

1. An electronic attestation of attributes shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

2. A qualified electronic attestation of attributes shall have the same legal effect as lawfully issued attestations in paper form.

3. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.

Article 45b

Electronic attestation of attributes in public services

When an electronic identification using an electronic identification means and authentication is required under national law to access an online service provided by a public sector body, person identification data in the electronic attestation of attributes shall not substitute electronic identification using an electronic identification means and authentication for electronic identification unless specifically allowed by the Member State or the public sector body. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.

Article 45c

Requirements for qualified attestation of attributes

1. Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V. A qualified electronic attestation of attributes shall be

www.parlament.gv.at

deemed to be compliant with the requirements laid down in Annex V, where it meets the standards referred to in paragraph 4.

2. Qualified electronic attestations of attributes shall not be subject to any mandatory requirement in addition to the requirements laid down in Annex V.

3. Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

4. Within 6 months of the entering into force of this Regulation, the Commission shall establish reference numbers of standards for qualified electronic attestations of attributes by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).

Article 45d

Verification of attributes against authentic sources

1. Member States shall ensure that, at least for the attributes listed in Annex VI, wherever these attributes rely on authentic sources within the public sector, measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the attribute directly against the relevant authentic source at national level or via designated intermediaries recognised at national level in accordance with national or Union law.

2. Within 6 months of the entering into force of this Regulation, taking into account relevant international standards, the Commission shall set out the minimum technical specifications, standards and procedures with reference to the catalogue of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).

Article 45e

Issuing of electronic attestation of attributes to the European Digital Identity Wallets

Providers of qualified electronic attestations of attributes shall provide an interface with the European Digital Identity Wallets issued in accordance in Article 6a.

Article 45f

Additional rules for the provision of electronic attestation of attributes services

1. Providers of qualified and non-qualified electronic attestation of attributes services shall not combine personal data relating to the provision of those services with personal data from any other services offered by them.

2. Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held.

3. Personal data relating to the provision of qualified electronic attestation of attributes services shall be kept physically and logically separate from any other data held.

www.parlament.gv.at

4. Providers of qualified electronic attestation of attributes' services shall provide such services under a separate legal entity.

SECTION 10

QUALIFIED ELECTRONIC ARCHIVING SERVICES

Article 45g

Qualified electronic archiving services

A qualified electronic archiving service for electronic documents may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the electronic document beyond the technological validity period.

Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for electronic archiving services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 11

ELECTRONIC LEDGERS

Article 45h

Legal effects of electronic ledgers

1. An electronic ledger shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.

2. A qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger.

Article 45i

Requirements for qualified electronic ledgers

1. Qualified electronic ledgers shall meet the following requirements:

   (a) they are created by one or more qualified trust service provider or providers;

   (b) they ensure the uniqueness, authenticity and correct sequencing of data entries recorded in the ledger;

   (c) they ensure the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry;

   (d) they record data in such a way that any subsequent change to the data is immediately detectable.

2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger meets the standards referred to in paragraph 3.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the processes of execution and registration of a set of data into, and the creation, of a qualified electronic ledger. Those implementing

www.parlament.gv.at

acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(40) The following Article 48a is inserted:

'*Article 48a*

Reporting requirements

1. Member States shall ensure the collection of statistics in relation to the functioning of the European Digital Identity Wallets and the qualified trust services.

2. The statistics collected in accordance with paragraph 1, shall include the following:

   (a) the number of natural and legal persons having a valid European Digital Identity Wallet;

   (b) the type and number of services accepting the use of the European Digital Wallet;

   (c) incidents and down time of the infrastructure at national level preventing the use of Digital Identity Wallet Apps.

3. The statistics referred to in paragraph 2 shall be made available to the public in an open and commonly used, machine-readable format.

4. By March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.';

(41) Article 49 is replaced by the following:

'*Article 49*

Review

1. The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council within 24 months after its entering into force. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal for amendment of this Regulation.

2. The evaluation report shall include an assessment of the availability and usability of the identification means including European Digital Identity Wallets in scope of this Regulation and assess whether all online private service providers relying on third party electronic identification services for users authentication, shall be mandated to accept the use of notified electronic identification means and European

3. In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.

(42) Article 51 is replaced by the following:

'*Article 51*

Transitional measures

www.parlament.gv.at

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall continue to be considered as qualified electronic signature creation devices under this Regulation until [date – OJ please insert period of four years following the entry into force of this Regulation].

2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until [date – PO please insert a period of four years following the entry into force of this Regulation].'.

(43) Annex I is amended in accordance with Annex I to this Regulation;

(44) Annex II is replaced by the text set out in Annex II to this Regulation;

(45) Annex III is amended in accordance with Annex III to this Regulation;

(46) Annex IV is amended in accordance with Annex IV to this Regulation;

(47) a new Annex V is added as set out in Annex V to this Regulation;

(48) a new Annex VI is added to this Regulation.

Article 2

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

www.parlament.gv.at

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Regulation of the European Parliament and of the Council on a framework for the European Digital Identity, amending the eIDAS regulation

1.2. Policy area(s) concerned

Policy area: Internal Market

Europe fit for a digital age

1.3. The proposal/initiative relates to:

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[28]

☑**the extension of an existing action**

☐ **a merger or redirection of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

The general objective of this initiative 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. This objective feeds into the strategic objectives set out in the Communication "Shaping Europe's digital future".

1.4.2. Specific objective(s)

Specific objective No 1

To provide access to trusted and secure digital identity solutions that can be used across borders, meeting user expectations and market demand;

Specific objective No 2

Ensure that public and private services can rely on trusted and secure digital identity solutions across borders;

Specific objective No 3

Provide citizens full control of their personal data and assure their security when using digital identity solutions;

Specific objective No 4

Ensure equal conditions for the provision of qualified trust services in the EU and their acceptance.

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

[28] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

www.parlament.gv.at

Overall, the biggest expected beneficiaries of the initiative are end users/citizens, online service providers, Wallet App providers and public and private providers of digital identity services. The initiative is expected to provide access to trusted and secure digital identity solutions that can be used cross borders, meeting user expectations and market demand; to ensure that public and private services can rely on trusted and secure digital identity solutions cross-border; to provide citizens full control of their personal data and assure their security when using digital identity solutions; and to ensure equal conditions for the provision of qualified trust services in the EU and their acceptance.

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).

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 and businesses.

In terms of economic growth it is expected that the introduction of a standard-based system will reduce uncertainty for market actors, and is also expected to have a positive impact on innovation.

And importantly, it is expected to provide 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, some citizens with disabilities, often those with reduced mobility, or living in rural areas may have lower access to services that normally require physical presence if not delivered locally.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Monitoring and evaluation aspect and relevant objectives	Indicator	Responsibility for collection	Source(s)
Application			
Provide access to eID means for all EU citizens	Number of European citizens and businesses issued with notified eID-s / European Digital Identity Wallets and number of issued identity credentials (attestations of attributes) .	European Commission and National Competent Authorities (NCA)	Annual survey/M&E data collected by NCAs

www.parlament.gv.at

Provide access to eID means for all EU citizens	Number of European citizens and businesses actively using notified eID-s / European Digital Identity Wallets and identity credentials (attestations of attributes)	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 / European Digital Identity Wallets and identity credentials (attestations of attributes)	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 / European Digital Identity Wallets and identity credentials (attestations of attributes) (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 attestation of attributes services meeting standards for integration into the European Digital identity Wallet	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	% of enterprises having e-commerce sales of goods or services	European Commission	Eurostat

www.parlament.gv.at

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	annual survey
Provide access to eID means for all EU citizens	% of individuals doing e-commerce % of individuals accessing online public services	European Commission	Eurostat

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

This Regulation shall be binding in its entirety and directly applicable in all Member States. Member States will be obliged to isse a European Digital Identity Wallet within 24-48 months (indicatively) of the adoption of the regulation. The Commission will be empowered to adopt implementing acts laying down the technical specifications and reference standards for the technical architecture of the European Digital Identity framework within 12-24 months (indicatively) of the adoption of the regulation.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

Reasons for action at European level (ex-ante)

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.

Expected generated Union added value (ex-post)

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

www.parlament.gv.at

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.

1.5.3. Lessons learned from similar experiences in the past

The eIDAS Regulation (Regulation 910/2014) (eIDAS) is the only cross-border framework for trusted electronic identification (eID) of natural and legal persons, and trust services. 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% 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. 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, 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 .

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 . 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.

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The initiative supports the European recovery effort by providing citizens and businesses the with tools necessary, e.g. convenient eID and trust services to help them conduct their daily activities online in a trusted and secure way. Hence, it is fully in line with the objectives of the MFF.

Operational expenditure is to be financed under DEP SO5. Procurement contracts supporting the development of standards and technical specifications, as well as the cost of maintaining the building blocks of the eID and trust services are estimated at up to 3-4MEURO annually. Exact allocation of this budget need is to be decided at the definition of future work programmes. Grants supporting the connection of

www.parlament.gv.at

public and private services to the eID ecosystem would greatly support reaching the objectives of the proposal. The cost for a service provider to integrate the necessary API of the eID Wallet is estimated at around 25.000 EURO as a one-off cost per provider. If available, once the distribution of budget for the next work programme is being discussed, budget for grants of up to 0.5MEUR / Member State would support the connection of a critical mass of services.

Expert group meetings related to the development of the implementing acts will be charged to the administrative part of DEP for a total amount of up to 0.5MEURO.

Synergies with other instruments

This initiative 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 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 .

The initiative 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. 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. 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 security coordination, such as the possible development of a European Social Security Pass which could build on the trust anchors offered by the notified identities under eIDAS.

This initiative supports the implementation of GDPR (2016/679) by putting the user in control over how the personal data is being used. It provides a high level of complementarity with the new Cybersecurity Act and its common cybersecurity certification schemes. 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 Single Digital Gateway Regulation (SDGR) has also important touchpoints and is in line with this initiative. SDGR’s 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. This initiative provides foundational elements to support the objectives of making the once only principle operational under the Single Digital Gateway.

www.parlament.gv.at

Furthermore, there is coherence with the European Strategy for Data and the proposed Regulation on European Data Governance, 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.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The initiative will build on the building blocks for eID and trust services that were developed under the CEF programme, and which are being integrated into DEP.

Member States can furthermore ask for financing for setting up/improving the infrastructure necessary from the RRF.

www.parlament.gv.at

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☑ **unlimited duration**

Implementation with a start-up period from YYYY to YYYY,

followed by full-scale operation.

1.7. Management mode(s) planned[29]

☑ **Direct management** by the Commission

☑ by its departments, including by its staff in the Union delegations;

☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

☐ third countries or the bodies they have designated;

☐ international organisations and their agencies (to be specified);

☐ the EIB and the European Investment Fund;

☐ bodies referred to in Articles 70 and 71 of the Financial Regulation;

☐ public law bodies;

☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

If more than one management mode is indicated, please provide details in the 'Comments' section.

Comments

[…]
[…]

[29] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

www.parlament.gv.at

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Regulation will be reviewed for the first time two years after its full application and then every four years. The Commission must report on the findings to the European Parliament and to the Council.

Moreover, in the context of the application of the measures, Member States shall collect statistics in relation to the use and the functioning of the European Digital Identity Wallet and qualified trust services. The statistics shall be collected in a report which shall be submitted to the Commission on an annual basis.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

The Regulation establishes more harmonised rules for the provision of eID and trust services in the internal market while ensuring the respect of trust and users' control over their own data. These new rules require the development of technical specifications and standards, and supervision and coordination of the activities of national authorities. In addition, the related building blocks for eID, eSignature etc will be managed and provided under DEP. There is also a need to take into consideration the resources needed to communicate and negotiate agreement with third countries on mutual recognition of trust services.

In order to face these tasks, it is necessary to appropriately resource the Commission's services. The enforcement of the new Regulation is estimated to require 11 FTEs; 4-5 FTEs for legal work, 4-5 FTEs for focusing on the technical work, and 2 FTE for coordination and international outreach and administrative support.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

One of the main issues leading to shortcomings of the current legislative framework is the lack of harmonisation of national systems. To overcome this problem in the current initiative, there will be a heavy reliance on reference standards and technical specifications to be defined in implementing acts.

The Commission will be supported by an expert group in the development of these implementing acts. Furthermore, the Commission will work together with Member States already now to agree on the technical nature of the future system, to prevent further fragementation during the negoitation of the proposal.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

For the meeting expenditure of the expert group, given the low value per transaction (e.g. refunding travel costs for a delegate for a meeting if the meeting is physical), standard internal control procedures seem sufficient.

www.parlament.gv.at

Also for pilot projects to be carried out under DEP, normal DG CNECT standard procedures should be sufficient.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

The existing fraud prevention measuers applicable to the Commission will cover the additional appropriations necessary for this Regulation.

www.parlament.gv.at

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[30]	from EFTA countries[31]	from candidate countries[32]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
2	02 04 05 01 deployment	Diff./	YES	NO	/NO	NO
2	02 01 30 01 support expenditure for the Digital Europe Programme	ND				
7	20 02 06 Administrative expenditure	ND	NO			

New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
	[XX.YY.YY.YY]		YES/NO	YES/NO	YES/NO	YES/NO

[30] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[31] EFTA: European Free Trade Association.

[32] Candidate countries and, where applicable, potential candidates from the Western Balkans.

www.parlament.gv.at

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

☐ The proposal/initiative does not require the use of operational appropriations

☑ The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	2

DG: CNECT			Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**		**TOTAL**
○ Operational appropriations				The allocation of budget will be decided during the formulation of the work programmes. Numbers indicated are the minimum needed for maintenance and upgrade[33].						
Budget line[34] 02 04 05	Commitments	(1a)	2.000	4.000	4.000	4.000	4.000	4.000		**22.000**
	Payments	(2a)	1.000	3.000	4.000	4.000	4.000	4.000	2.000	**22.000**
Budget line	Commitments	(1b)								
	Payments	(2b)								
Appropriations of an administrative nature financed from the envelope of specific programmes[35]										
Budget line 02 01 03 01		(3)	**0.048**	**0.144**	**0.144**	**0.072**	**0.072**	**0.072**		**0.552**
TOTAL appropriations for DG CNECT	Commitments	=1a+1b +3	2.048	4.144	4.144	4.072	4.072	**4.072**		**22.552**
	Payments	=2a+2b	1.048	3.144	4.144	4.072	4.072	**4.072**	**2.000**	**22.552**

33 Should the actual cost exceed the amounts indicated, the costs will be financed by 02 04 05 01

34 According to the official budget nomenclature.

35 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

www.parlament.gv.at

		+3								

○ TOTAL operational appropriations	Commitments	(4)	2.000	4.000	4.000	4.000	4.000	4.000		**22.000**
	Payments	(5)	1.000	3.000	4.000	4.000	4.000	4.000	2.000	**22.000**
○ TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)	**0.048**	**0.144**	**0.144**	**0.072**	**0.072**	**0.072**		**0.552**
TOTAL appropriations under HEADING 2 of the multiannual financial framework	Commitments	=4+ 6	2.048	4.144	4.144	4.072	4.072	**4.072**		**22.552**
	Payments	=5+ 6	0.048	4.144	4.144	4.072	4.072	**4.072**	**2.000**	**22.552**

www.parlament.gv.at

Heading of multiannual financial framework	7	'Administrative expenditure'

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
DG: CNECT								
○ Human resources		0.776	1.470	1.470	1.470	1.470	1.318	**7.974**
○ Other administrative expenditure		0.006	0.087	0.087	0.087	0.016	0.016	**0.299**
TOTAL DG CNECT	Appropriations	0.782	1.557	1.557	1.557	1.486	1.334	**8.273**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	0.782	1.557	1.557	1.557	1.486	1.334	**8.273**

thEUR million (to three decimal places)

		Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**		**TOTAL**
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments	2.830	5.701	5.701	5.629	5.558	5.408		**30.825**
	Payments	1.830	4.701	5.701	5.629	5.558	5.406	2.000	**30.825**

www.parlament.gv.at

3.2.2. Estimated output funded with operational appropriations

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
	Type [36]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 [37] …	To provide access to trusted and secure digital identity solutions that can be used across borders, meeting user expectations and market demand															
Annual surveys/studies			1	0.050	1	0.050	1	0.050.	1	0.050	1	0.050	1	0.050	6	0.300
Subtotal for specific objective No 1			1	0.050	1	0.050	1	0.050	1	0.050	1	0.050	1	0.050	6	0.300
SPECIFIC OBJECTIVE No 2 ...	Enusre that public and private services can rely on trusted and secure digital identity solutions across borders;															
Surveys/studies			1	0.050	1	0.050	1	0.050.	1	0.050	1	0.050	1	0.050	6	0.300
Subtotal for specific objective No 2			1	0.050	1	0.050	1	0.050	1	0.050	1	0.050	1	0.050	6	0.300
SPECIFIC OBJECTIVE No 3 ...	Provide citizens full control of their personal data and assure their security when using digital identity solutions;;															
Surveys/studies			1	0.050	1	0.050	1	0.050.	1	0.050	1	0.050	1	0.050	6	0.300
Subtotal for specific objective No 3			1	0.050	1	0.050	1	0.050	1	0.050	1	0.050	1	0.050	6	0.300
SPECIFIC OBJECTIVE No 4 ...	Ensure equal conditions for the provision of qualified trust services in the EU and their acceptance.															
Surveys/studies			1	0.050	1	0.050	1	0.050.	1	0.050	1	0.050	1	0.050	6	0.300
Subtotal for specific objective No 4			1	0.050	1	0.050	1	0.050	1	0.050	1	0.050	1	0.050	6	0.300

[36] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

[37] As described in point 1.4.2. 'Specific objective(s)…'

www.parlament.gv.at

TOTAL	4	0.200	4	0.200	4	0.200	4	0.200	4	0.200	4	0.200	24	1.200

www.parlament.gv.at

3.2.3. Summary of estimated impact on administrative appropriations

☐ The proposal/initiative does not require the use of appropriations of an administrative nature

☑ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
HEADING 7 of the multiannual financial framework							
Human resources	0.776	1.470	1.470	1.470	1.470	1.318	**7.974**
Other administrative expenditure	0.006	0.087	0.087	0.087	0.0162	0.0162	**0.299**
Subtotal HEADING 7 of the multiannual financial framework	0.782	1.557	1.557	1.557	1.486	1.334	**8.273**

Outside HEADING 7[38] **of the multiannual financial framework**							
Human resources							
Other expenditure of an administrative nature Put the admin costs under DEP	0.048	0.144	0.144	0.072	0.072	**0.072**	**0,552**
Subtotal outside HEADING 7 of the multiannual financial framework	0.048	0.144	0.144	0.072	0.072	**0.072**	**0,552**

TOTAL	**0.830**	**1.701**	**1.701**	**1.629**	**1.558**	**1.406**	**8.825**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

[38] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

www.parlament.gv.at

3.2.4. Estimated requirements of human resources

☐ The proposal/initiative does not require the use of human resources.

☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

		Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**
20 01 02 01 (Headquarters and Commission's Representation Offices)		4	8	8	8	8	7
20 01 02 03 (Delegations)							
01 01 01 01 (Indirect research)							
01 01 01 11 (Direct research)							
Other budget lines (specify)							
20 02 01 (AC, END, INT from the 'global envelope')		2	3	3	3	3	3
20 02 03 (AC, AL, END, INT and JPD in the delegations)							
XX 01 xx **yy zz** [39]	- at Headquarters						
	- in Delegations						
01 01 01 02 (AC, END, INT - Indirect research)							
01 01 01 12 (AC, END, INT - Direct research)							
Other budget lines (specify)							
TOTAL		**6**	**11**	**11**	**11**	**11**	**10**

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	Officials will mainly carry out legal work, coordination activities and negotiations with 3rd countries and bodies related to mutual recognition of trust services.
External staff	National experts should support with the technical and functional set-up of the system. AC should also support with technical tasks including management of the building blocks.

[39] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

www.parlament.gv.at

3.2.5. Compatibility with the current multiannual financial framework

The proposal/initiative:

☑ can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts. Please provide an excel table in the case of major reprogramming.

☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used.

☐ requires a revision of the MFF.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.6. Third-party contributions

The proposal/initiative:

☑ does not provide for co-financing by third parties

☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **N**[40]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[40] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

www.parlament.gv.at

3.3. Estimated impact on revenue

☑ The proposal/initiative has no financial impact on revenue.

☐ The proposal/initiative has the following financial impact:

☐ on own resources

☐ on other revenue

please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[41]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For assigned revenue, specify the budget expenditure line(s) affected.

[…]

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[…]

[41] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

www.parlament.gv.at

ANNEX
to the LEGISLATIVE FINANCIAL STATEMENT

Name of the proposal/initiative:

Proposal for a Regulation on a framework for the European Digital Identity amending the eIDAS regulation

1. NUMBER AND COST OF HUMAN RESOURCES CONSIDERED NECESSARY

2. COST OF OTHER ADMINISTRATIVE EXPENDITURE

3. TOTAL ADMINISTRATIVE COSTS

4. METHODS OF CALCULATION USED FOR ESTIMATING COSTS

4.1. Human resources

4.2. Other administrative expenditure

This annex must accompany the legislative financial statement when the inter-services consultation is launched.

The data tables are used as a source for the tables contained in the legislative financial statement. They are strictly for internal use within the Commission.

www.parlament.gv.at

(1) Cost of human resources considered necessary

☐ The proposal/initiative does not require the use of human resources

☑ The proposal/initiative requires the use of human resources, as explained below:

EUR million (to three decimal places)

www.parlament.gv.at

HEADING 7 of the multiannual financial framework		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)															
20 01 02 01 - Headquarters and Representation offices	AD	4	608	7	1.064	7	1.064	7	1.064	7	1.064	6	912	38	5.776
	AST	0	-	1	152	1	152	1	152	1	152	1	152	5	760
20 01 02 03 - Union Delegations	AD														
	AST														
External staff [1]															
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC	1	82	1	82	1	82	1	82	1	82	1	82	6	492
	END	1	86	2	172	2	172	2	172	2	172	2	172	11	946
	INT														
20 02 03 – External personnel - Union Delegations	AC														
	AL														
	END														
	INT														
	JPD														
Other HR related budget lines (*specify*)															
Subtotal HR – HEADING 7		6	776	11	1.470	11	1.470	11	1.470	11	1.470	10	1.318	60	7.974

www.parlament.gv.at

4.3. The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

4.4.

4.5.

Outside HEADING 7 of the multiannual financial framework			**Year 2022**		**Year 2023**		**Year 2024**		**Year 2025**		**Year 2026**		**Year 2027**		**TOTAL**	
			FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
01 01 01 01 Indirect Research[42] 01 01 01 11 Direct Research Other (please specify)		AD														
		AST														
External staff from operational appropriations (former 'BA' lines).	- at Headquarters	AC														
		END														
		INT														
	- in Union delegations	AC														
		AL														
		END														
		INT														
		JPD														
01 01 01 02 Indirect Research 01 01 01 12 Direct research Other (please specify)[43]		AC														
		END														
		INT														
Other budget lines HR related (*specify*)																
Subtotal HR – Outside HEADING 7																

[42] Please choose the relevant budget line, or specify another if necessary; in case more budget lines are concerned, staff should be differentiated by each budget line concerned

[43] Please choose the relevant budget line, or specify another if necessary; in case more budget lines are concerned, staff should be differentiated by each budget line concerned

www.parlament.gv.at

Total HR (all MFF Headings)		6	0.776	11	1.470	11	1.470	11	1.470	11	1.470	10	1.318	60	7.974

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

www.parlament.gv.at

4.6. Cost of other administrative expenditure

4.7. ☐ The proposal/initiative does not require the use of administrative appropriations

4.8. ☑ The proposal/initiative requires the use of administrative appropriations, as explained below:

EUR million (to three decimal places)

HEADING 7 of the multiannual financial framework	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	Total
At headquarters or within EU territory:							
20 02 06 01 - Mission and representation expenses	0,006	0,015	0,015	0,015	0,015	0,015	**0.081**
20 02 06 02 - Conference and meeting costs							
20 02 06 03 - Committees[44]		0.072	0.072	0.072	0.0012	0.012	**0.218**
20 02 06 04 Studies and consultations							
20 04 – IT expenditure (corporate)[45]							
Other budget lines non-HR related (*specify where necessary*)							
In Union delegations							
20 02 07 01 - Missions, conferences and representation expenses							
20 02 07 02 - Further training of staff							
20 03 05 – Infrastructure and logistics							
Other budget lines non-HR related (*specify where necessary*)							
Subtotal Other - HEADING 7 of the multiannual financial framework	0.006	0.087	0.087	0.087	0.016	0.016	**0.299**

[44] Specify the type of committee and the group to which it belongs.

[45] The opinion of DG DIGIT – IT Investments Team is required (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020, page 7)

www.parlament.gv.at

EUR million (to three decimal places)

Outside HEADING 7 of the multiannual financial framework	**Year 2022**	**Year 2023**	**Year 2024**	**Year 2025**	**Year 2026**	**Year 2027**	**Total**
Expenditure on technical and administrative assistance (not including external staff) from operational appropriations (former 'BA' lines):	0.048	0.144	0.144	0.072	0.072	0.072	**0.552**
- at Headquarters							
- in Union delegations							
Other management expenditure for research							
Policy IT expenditure on operational programmes[46]							
Corporate IT expenditure on operational programmes[47]							
Other budget lines non-HR related (*specify where necessary*)							
Sub-total Other – Outside HEADING 7 of the multiannual financial framework	0.048	0.144	0.144	0.072	0.072	0.072	**0.552**
Total Other admin expenditure (all MFFHeadings)	0.054	0.231	0.231	0.159	0.088	0.088	0.851

[46] The opinion of DG DIGIT – IT Investments Team is required (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020, page 7)

[47] This item includes local administrative systems and contributions to the co-financing of corporate IT systems (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020)

www.parlament.gv.at

5. TOTAL ADMINISTRATIVE COSTS (ALL HEADINGS MFF)

EUR million (to three decimal places)

Summary	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	Total
Heading 7 - Human Resources	0.776	1.470	1.470	1.470	1.470	1.318	**7.974**
Heading 7 – Other administrative expenditure	0.006	0.087	0.087	0.087	0.016	0.016	**0.218**
Sub-total Heading 7							
Outside Heading 7 – Human Resources							
Outside Heading 7 – Other administrative expenditure	0.048	0.144	0.144	0.072	0.072	0.072	**0.552**
Sub-total Other Headings							
1. TOTAL 2. HEADING 7 and Outside HEADING 7	0.830	1.701	1.701	1.629	1.558	1.406	**8.825**

(1) The administrative appropriations required will be met by the appropriations which are already assigned to management of the action and/or which have been redeployed, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of existing budgetary constraints.

www.parlament.gv.at

6. METHODS OF CALCULATION USED TO ESTIMATE COSTS

(a) Human resources

This part sets out the method of calculation used to estimate the human resources considered necessary (workload assumptions, including specific jobs (Sysper 2 work profiles), staff categories and the corresponding average costs)

1.	**HEADING 7** of the multiannual financial framework
2.	NB: The average costs for each category of staff at Headquarters are available on BudgWeb:
3.	https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
4.	O Officials and temporary staff
5.	7 AD officials (including 1 from CNECT/F.3 in 2023-2024) x 152.000 euro / year in 2023-2027 (half of that in 2022 due to adoption expected mid 2022);
6.	1 AST official x 152.000 euro / year in 2023-2027 (half of that in 2022 due to adoption expected mid 2022)
7.	
8.	O External staff
9.	AC: 1 x 82.000 euro / year in 2023-2027 (half of that in 2022 due to adoption expected mid 2022) (indexation factor applied);
10.	END 2 x 86.000 euro / year in 2023-2027 (half of that in 2022 due to adoption expected mid 2022) (indexation factor applied);
11.	

12.	**Outside HEADING 7** of the multiannual financial framework
13.	O Only posts financed from the research budget
14.	
15.	O External staff
16.	

7. OTHER ADMINISTRATIVE EXPENDITURE

Give details of the method of calculation used for each budget line and in particular the underlying assumptions (e.g. number of meetings per year, average costs, etc.)

17.	**HEADING 7** of the multiannual financial framework
18.	Bi-monthly committee meetings x 12.000 euro / meeting 2022-2024 to adopt implementing acts. After that annual committee meetings for adopting updated implementing acts.
19.	Mission are mainly Luxembourg-Brussels travels but also to attend conferences, meetings with Member States and other stakeholders.
20.	

21.	**Outside HEADING 7** of the multiannual financial framework
22.	Expert group meetings are to be charged to the administrative line of DEP.
23.	It is expected to hold monthly meetings (à 12.000 EURO) during the preparation of implementing act (mid 2022-2024) and outside of that period of time, bi-monthly meetings are foreseen to ensure EU-wide coordination related to technical implementation.
24.	

www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 3.6.2021
COM(2021) 281 final

ANNEX

ANNEX

to the proposal for a

Regulation of the European Parliament and of the Council

amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

www.parlament.gv.at

ANNEX I

In Annex I, point (i) is replaced by the following:

‘(i) the information, or the location of the services that can be used to enquire, about the validity status of the qualified certificate;’.

ANNEX II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

   (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;

   (b) the electronic signature creation data used for electronic signature creation can practically occur only once;

   (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;

   (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

ANNEX III

In Annex III, point (i) is replaced by the following:

‘(i) the information, or the location of the services that can be used to enquire, about the validity status of the qualified certificate;’.

ANNEX IV

In Annex IV, point (j) is replaced by the following:

‘(j) the information, or the location of the certificate validity status services that can be used to enquire, about the validity status of the qualified certificate.’.

ANNEX V

REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES

Qualified electronic attestation of attributes shall contain:

(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and:

– for a legal person: the name and, where applicable, registration number as stated in the official records,

– for a natural person: the person's name;

(c) a set of data unambiguously representing the entity to which the attested attributes is referring to; if a pseudonym is used, it shall be clearly indicated;

(d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;

(e) details of the beginning and end of the attestation's period of validity;

(f) the attestation identity code, which must be unique for the qualified trust service provider and if applicable the indication of the scheme of attestations that the attestation of attributes is part of;

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (f) is available free of charge;

(i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation.

ANNEX VI

MINIMUM LIST OF ATTRIBUTES

Further to Article 45d, Member States shall ensure that measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with national or Union law and in cases where these attributes rely on authentic sources within the public sector:

1. Address;
2. Age;
3. Gender;
4. Civil status;
5. Family composition;
6. Nationality;
7. Educational qualifications, titles and licenses;
8. Professional qualifications, titles and licenses;
9. Public permits and licenses;
10. Financial and company data.