Council of the European Union
General Secretariat

Brussels, 01 February 2022

WK 1440/2022 INIT

LIMITE

TELECOM

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	European Digital Identity : IE comments (doc. 9471/21)

Delegations will find in the annex IE comments on European Digital identity.

Deadline: ***31 January 2022***

Important: In order to guarantee that your comments appear accurately, please do not modify the table format by adding/removing/adjusting/merging/splitting cells and rows. This would hinder the consolidation of your comments. When adding new provisions, please use the free rows provided for this purpose between the provisions. You can add multiple provisions in one row, if necessary, but do not add or remove rows. For drafting suggestions (2nd column), please copy the relevant sentence or sentences from a given paragraph or point into the second column and add or remove text. Please do not use track changes, but highlight your additions in yellow or use ~~strikethrough~~ to indicate deletions. You do not need to copy entire paragraphs or points to indicate your changes, copying and modifying the relevant sentences is sufficient. For comments on specific provisions, please insert your remarks in the 3rd column in the relevant row. If you wish to make general comments on the entire proposal, please do so in the row containing the title of the proposal (in the 3rd column).

Commission proposal	Drafting Suggestions	Comments
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,		

Commission proposal	Drafting Suggestions	Comments
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[1],		
Acting in accordance with the ordinary legislative procedure,		
Whereas:		
(1) The Commission Communication of 19 February 2020, entitled "Shaping Europe's Digital Future"[2] announces a revision of Regulation (EU) No 910/2014 of the European Parliament and of the Council with the aim of		

[1] OJ C , , p. .
[2] COM/2020/67 final

Commission proposal	Drafting Suggestions	Comments
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[3], 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"[4] sets the objective of a Union framework which, by 2030, leads to wide deployment of a trusted,		

[3] https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/
[4] COM/2021/118 final/2

Commission proposal	Drafting Suggestions	Comments
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 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		

Commission proposal	Drafting Suggestions	Comments
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.		

Commission proposal	Drafting Suggestions	Comments
(6) Regulation (EU) No 2016/679[5] 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		

[5] 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

Commission proposal	Drafting Suggestions	Comments
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		Online and Offline Authentication will be critially important as will the security of the

Commission proposal	Drafting Suggestions	Comments
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 under this Regulation. The European Digital Identity Wallets should also allow users to create and use qualified electronic signatures and seals		Digital wallet and its ability to use trusted storage. Care must also be taken to ensure consumers are not precluded from taking advantage of the European Digital Identity Wallet through the need to access this app by the possession of flag ship smartphones.

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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[6]. Such certification should be		

[6] 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

Commission proposal	Drafting Suggestions	Comments
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.		

Commission proposal	Drafting Suggestions	Comments
(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.		
(13) Regulation (EU) No 2019/1157[7] strengthens the security of identity cards with enhanced security features by August 2021.		It should be acknowledged that not all Member States issue identity cards and that this represents a challenge for those Member States

[7] 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).

Commission proposal	Drafting Suggestions	Comments
Member States should consider the feasibility of notifying them under electronic identification schemes to extend the cross-border availability of electronic identification means.		in order to reach the high levels of assurance required in relation to eID.
(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.		The process of notification should be simple and be reproducable to provide consistent peer reviews. This is critially important to the success of notfication alongside ecouraging the participation of the private sector.
(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		An alternative peer review process for the notification of electronic identiity schemes is important where innovative electronic identity solutions are being proposed (especially non identity card based solutions)

Commission proposal	Drafting Suggestions	Comments
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.		Member States should be able to benefit from new flexible tools to ensure compliance with the requirements of the regulation, but this objective is entirely dependent on the streamlining of the peer review and notification processess for those objectives to be realised.

Commission proposal	Drafting Suggestions	Comments
(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		We see identity matching as a significant blocker to eIDAS uptake and a barrier towards the acceptance of eID by relying parties. The expansion of the minimium data set is welcomed but the use of unique and persistent identifiers is more important to reduce the burden on relying parties/central identity matching services.

Commission proposal	Drafting Suggestions	Comments
legally identify the user upon his/her request in a unique and persistent way.		
(18) In line with Directive (EU) 2019/882[8], 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 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.		

[8] 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).

Commission proposal	Drafting Suggestions	Comments
(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],		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		We request clarification on the inclusion of threats which are not part of the mandatory notification process as set out in the Council general approach on NIS2.

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
affect the obligation to notify personal data breaches under Regulation (EU) 2016/679.		
(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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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 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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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.		Privacy by design and privacy by default including selective disclosure, will be important to build trust in the European Digital Identity Wallet, but also to put the citizen in contol of their data allowing them make informed decisions about who they share data with, especially with the private sector.
(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		

Commission proposal	Drafting Suggestions	Comments
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		As identity, authentication and the ability of citizens to hold a wide range of attributes or credentials are core wallet functionalities of the wallet, the finacial services sector should be accommodated directly.

Commission proposal	Drafting Suggestions	Comments
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		QWACs have been proposed as a new and emerging standard for Trust Services. We understand that the original objective of introducing a new standard appears to be twofold: Firstly, by providing a legal framework to stimulate Trust Service provision within Europe thereby creating a new market for higher standard "Qualified" Trust Services (QTS). The second objective was to specifically establish and promote the use of QWACs as a new standard for website authentication originating in Europe which would be adopted and accepted by the CA/Browser forum. These objectives are clearly in line with the eIDAS Regulation and the intentions of expanding the Digital Single Market (DSM). We feel however, that given that the uptake of QWACs has been below what was expected, the

Commission proposal	Drafting Suggestions	Comments
Regulation (EU) No 910/2014. They should recognise and display Qualified certificates for website 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.		technical proposal of decoupling TLS whose role is to support secure communication and authentication in its primary context from the QWACs, in our opinion neither establishes QWACs as a worthwhile standard nor will drive its adoption. Furthermore, it is difficult for us to see specific use case for non TLS QWACs. For these reasons, we do not see a need for the proposed change.
(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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
Instruments Directive[9], the Payment Services Directive[10] and the future Markets in Crypto Assets Regulation[11].		
(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 coordinated approach towards a European		

9 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.*

10 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.*

11 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.

Commission proposal	Drafting Suggestions	Comments
Digital Identity Framework][12] 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		

[12] [insert reference once adopted]

Commission proposal	Drafting Suggestions	Comments
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[13].		
(38) Regulation (EU) 910/2014 should therefore be amended accordingly,		
HAVE ADOPTED THIS REGULATION:		
Article 1		
Regulation (EU) 910/2014 is amended as follows:		

[13] 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).

Commission proposal	Drafting Suggestions	Comments
(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		

Commission proposal	Drafting Suggestions	Comments
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 issued by Member States and to trust service providers that are established in the Union.’;		
(b) paragraph 3 is replaced by the following:		

Commission proposal	Drafting Suggestions	Comments
'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:		

Commission proposal	Drafting Suggestions	Comments
'(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:		

Commission proposal	Drafting Suggestions	Comments
(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;		Ireland suggests that certificates for website authentitication are not helpful in the security of the internet. The collaborative internet industry do not see it helpful to address this product within the European Legislation. Ireland would support deletion of Certificates for website authentication from the Regulation.
(c) the preservation of electronic signatures, seals or certificates related to those services;		
(d) the electronic archiving of electronic documents;		

Commission proposal	Drafting Suggestions	Comments
(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:		
‘(23a) ‘remote qualified signature creation device’ means a qualified electronic signature creation device where a qualified trust service provider generates, manages or duplicates the		We suggest that the intention of the article should be made clearer to show this is needed in order to meet the requirements of demonstrating sole control.

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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;		A European Digital Identity wallet could conceivably be both a product and a service, the text proposed should reflect this.
(43) 'attribute' is a feature, characteristic or quality of a natural or legal person or of an entity, in electronic form;		

Commission proposal	Drafting Suggestions	Comments
(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		

Commission proposal	Drafting Suggestions	Comments
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;		
(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		

Commission proposal	Drafting Suggestions	Comments
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.';		

Commission proposal	Drafting Suggestions	Comments
(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		

Commission proposal	Drafting Suggestions	Comments
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.		

Commission proposal	Drafting Suggestions	Comments
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 identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services;		

Commission proposal	Drafting Suggestions	Comments
(b) sign by means of qualified electronic signatures.		
4. Digital Identity Wallets shall, in particular:		
(a) provide a common interface:		The nature of the common interface is yet to be fully defined and requires further definitional work within the eIDAS experts group.
(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;		

Commission proposal	Drafting Suggestions	Comments
(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		It should be recognised that the assurance level of High is a significant barrier for Member States, especially those who do not have national identity card schemes.

Commission proposal	Drafting Suggestions	Comments
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;		

Commission proposal	Drafting Suggestions	Comments
(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		

Commission proposal	Drafting Suggestions	Comments
Digital Identity 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.		

Commission proposal	Drafting Suggestions	Comments
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.		At this early stage of wallet definition, this appears a very significant albeit important challenge to be overcome.
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		

Commission proposal	Drafting Suggestions	Comments
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.		In general this article, places a large obligation on Member States. It appears to imply major governance arrangements are required which will be a significant undertaking for Member States. As a result, we believe that there may be liability questions that arise which may not be fully understood until the implementing Act is defined. Further information about the governance arrangements anticipated is therefore needed. We also request clarity for which times the authentications needed will take place.
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		

Commission proposal	Drafting Suggestions	Comments
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		It is not obvious at this time, if there exists a cybersecurity scheme capable of certifying a digital wallet against. As such the impact on the

Commission proposal	Drafting Suggestions	Comments
(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 paragraphs 3, 4 and 5 in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.		timeframe required to certify a digital wallet is unknown. Certification of digital wallets are highly contingent on standards and criteria yet to be developed by unknown accredited bodies with the appropriate competence.
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.		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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:';		We note that the new mandatory requirement for member states to notify an eID (at a high level of assurance) is a significant new obligation for Member States.

Commission proposal	Drafting Suggestions	Comments
(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.		
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*		

Commission proposal	Drafting Suggestions	Comments
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.		We wish to know how will the suspension of the European Digital Identity Wallet be coordinated across Member States. It is currently unclear if ENISA will be tasked with this activity, and if there will be the need for a specific reporting tool to be used to notify any such breaches.
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		The security of the wallet is a core functionality, but what are the conditions required to re-establishing compromised wallets.

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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 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:		

Commission proposal	Drafting Suggestions	Comments
‘(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		We would be grateful for clarity as to the expectations of this article, especially regarding the requirements which the certifying body,

Commission proposal	Drafting Suggestions	Comments
		either public or private, need to meet in order to be qualified for certifying the conformity of the European Digital Identity Wallets.
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		

Commission proposal	Drafting Suggestions	Comments
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:		

Commission proposal	Drafting Suggestions	Comments
'Article 12b		
Cross-border reliance on European Digital Identity Wallets		The scope of this article seems to be very wide. Should the text reflect the need to recognise only approved cross border use cases?
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.		
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		

Commission proposal	Drafting Suggestions	Comments
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.		This article appears to be quite an aspirational requirement for the private sector, especially for the large platforms and can only be achieved through citizen support and demand for this functionality.
4. The Commission shall encourage and facilitate the development of self-regulatory		Acceptance and adoption in our view, will be achieved more through use cases which create

Commission proposal	Drafting Suggestions	Comments
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.		demand for digital services rather than through self regulation.
5. The Commission shall make an assessment within 18 months after deployment		

Commission proposal	Drafting Suggestions	Comments
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.		

Commission proposal	Drafting Suggestions	Comments
Article 12c		
Mutual recognition of other electronic identification means		The legal text appears to promote the recognition of a new wallet over the existing interoperability framework, thereby introducting the possibility of duplication. We are concerned therefore that the nature of this article will result in duplication of infrastructure and additional costs for Member States.
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		

Commission proposal	Drafting Suggestions	Comments
online service, provided that the following conditions are met:		
(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.		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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.		

Commission proposal	Drafting Suggestions	Comments
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 accessibility		

Commission proposal	Drafting Suggestions	Comments
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		We request clarification at as to what ‘significant’ means. If there is a breach of security or loss of integrity, then the relevant NIS authorities should know about it. Further, we wish that other supervisory bodies would be informed about breaches of security or loss of integrity in accordance with Article 19(2).

Commission proposal	Drafting Suggestions	Comments
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.’;		

Commission proposal	Drafting Suggestions	Comments
(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).';		We wish clarification on the proposal to use Implementing Acts to permit the Commission assign new tasks to Supervisory bodies as per Article 17(8). In addition, would it not be more useful for the tasks to be listed at this point?
(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:		

Commission proposal	Drafting Suggestions	Comments
'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 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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
'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.';		The conformity assessment body can only confirm that the requirements of the Regulation are being complied with. NIS competent authorities have supervisory and enforcement powers on qualified trust service povidiers as essential entities under Article 29 of NIS2. Such powers include requirements for auditing. The conformity assessment body cannot prejudice the rights of NIS competent authorities and therefore Article 18 of NIS2 is beyond the competence of the conformity assessment body.
(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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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:		
(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		

Commission proposal	Drafting Suggestions	Comments
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:		

Commission proposal	Drafting Suggestions	Comments
'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.		The request to carry out supervisory actions should specify those actions as set out in Articles 29 and 30 of NIS2. Feedback should be provided promptly after the completion of the specific supervisory actions. However, we suggest that a reference to 3 days may not be appropriate or sufficiently clear. If 3 calendar days is implied, how would this work during an extended holiday period? If 3 working days is implied, then the duration will depend on working days in the Member State concerned.

Commission proposal	Drafting Suggestions	Comments
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:		

Commission proposal	Drafting Suggestions	Comments
'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:		
'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:		

Commission proposal	Drafting Suggestions	Comments
(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';		

Commission proposal	Drafting Suggestions	Comments
(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:		

Commission proposal	Drafting Suggestions	Comments
'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		

Commission proposal	Drafting Suggestions	Comments
of that service, including any limitations on its use;’;		
(2) the new points (fa) and (fb) are inserted:		
‘(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:		This legislative proposal should not prejudice the NIS2 legislation. The measures are in addition to and not instead of those measures in Article 18 of NIS2.
(i) measures related to registration and on-boarding procedures to a service;		
(ii) measures related to procedural or administrative checks;		

Commission proposal	Drafting Suggestions	Comments
(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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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:		
‘6. Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish		

Commission proposal	Drafting Suggestions	Comments
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:		

Commission proposal	Drafting Suggestions	Comments
'*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:		

Commission proposal	Drafting Suggestions	Comments
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:		

Commission proposal	Drafting Suggestions	Comments
'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 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:		

Commission proposal	Drafting Suggestions	Comments
'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*		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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:		
‘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		

Commission proposal	Drafting Suggestions	Comments
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:		

Commission proposal	Drafting Suggestions	Comments
(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:		

Commission proposal	Drafting Suggestions	Comments
(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:		

Commission proposal	Drafting Suggestions	Comments
'*Article 45*		
Requirements for qualified certificates for website authentication		**Ireland would be pleased to see this article and QWACS removed from the trust services set out in this regulation. We feel that the browser industry are adept and managing the security aspects of internet web access. In particular, the development of the internet in a dynamic way has been based on collaboration between the industries, within the concept of multistakeholderism. Therefore, we feel that it is not necessary for the Commission to set out technical details on the operation of the internet in European legistlation.**
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		

Commission proposal	Drafting Suggestions	Comments
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.		**Ireland** recommends that the provisions in this subparagraph be deleted. They could be replaced with guidance to the effect that TSPs should meet industry best practices including meeting and exceeding the requirements of web-browsers. This will ensure that current security of web-browsers is maintained.
3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide the		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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 deemed to be compliant with		

Commission proposal	Drafting Suggestions	Comments
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).		

Commission proposal	Drafting Suggestions	Comments
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 proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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.		

Commission proposal	Drafting Suggestions	Comments
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.		

Commission proposal	Drafting Suggestions	Comments
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.		

Commission proposal	Drafting Suggestions	Comments
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;		

Commission proposal	Drafting Suggestions	Comments
(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 acts shall be adopted in		

Commission proposal	Drafting Suggestions	Comments
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;		

Commission proposal	Drafting Suggestions	Comments
(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*		

Commission proposal	Drafting Suggestions	Comments
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		

Commission proposal	Drafting Suggestions	Comments
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		
1. Secure signature creation devices of which the conformity has been determined in		

Commission proposal	Drafting Suggestions	Comments
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;		

Commission proposal	Drafting Suggestions	Comments
(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.		

Commission proposal	Drafting Suggestions	Comments
Done at Brussels,		
For the European Parliament For the Council		
The President The President		
	End	**End**