Working Party on Telecommunications and Information Society

Proposal for a Regulation of the European Parliament and the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Identity

German comments with regards to the third compromise proposal (doc: 11713/22)

A. General comments

Germany would like to thank the Presidency for the third compromise proposal. Germany supports the aim of the Presidency and the Commission to reach a General Approach as soon as possible. Nevertheless, in our view, there are still some serious issues left which should be looked at closely as the revision of the eIDAS Regulation is a very important legal act for a competitive European single digital market.

B. Specific Points

1. **Rec. (8a)**

   We suggest deletion of the recital. In our view, the main reason for a registration obligation is not the risk posed by online data transfers. The key reason is that registration provides an overview of the relying parties and services using the Wallet. Registration makes it significantly easier for supervisory authorities to intervene in case of security incidents, fraudulent use or other issues. This motivation also applies to a fully offline use of the Wallet – maybe even more, as it seems harder to supervise fully offline use scenarios where, except for the relying party and the user, nobody is aware of the transmission of personal identification data.

   We are therefore strongly in support for registration obligations for all relying parties. However, registration should be kept as simple as possible.

2. **Rec. (9)**

In our view, data protection should be mentioned here alongside security, as both must go hand in hand, as the Recital states itself. Therefore, we suggest the following drafting:

"(…) 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 data protection and security. (…) 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 data protection and security commensurate to the risks raised for the rights and freedoms of the natural persons, in line with Regulation (EU) 2016/679."

Is our understanding of the last, newly added sentence of this Recital correct that it would be up to the Member States to charge natural persons certain fees for using the Wallet?

3. **Rec. (10)**

Data protection should be mentioned here as well (see above). The provision should therefore read as follows:

"In order to achieve a high level of data protection, security and trustworthiness, this Regulation establishes the requirements for European Digital Identity Wallets (…)."

4. **Rec. (10a)**

The statements in recital 10a are inconsistent with Art. 24. There, "substantially plus" was deleted because of the vagueness, now it could be signed with it again via the indirection of the wallet.

5. **Rec. (11)**

With regards to this recital also both security and (data) protection should be mentioned here. The provision should therefore read as follows:

"European Digital Identity Wallets should ensure the highest level of protection and 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."

Furthermore, we suggest using GDPR terminology here (biometric data is a defined notion). Biometrics are an important authentication factor. However, given that the Identity Wallet should ensure the highest level of security, Biometrics should only be one authentication factors in a multiple factor authentication scheme that uses several factors from different categories. The current wording gives the impression that relying on biometrics alone as an authentication factor provides a sufficient level of security, which is not the case. The state of knowledge is that scanners in current smartphones are not able to have a high level of confidence while using biometrics. Also, the aspect of conscious authentication is not given (at least for facial biometrics). Therefore, the provision should read as follows:

" ~~Using biometrics~~ The processing of biometric data as an authentication element in multi-factor authentication 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 biometric~~s~~ data represents a unique characteristic of a person, the ~~use~~ processing of ~~biometrics~~ biometric data is only allowed under the exceptions of Article 9 (2) of Regulation (EU) 2016/679 and requires appropriate safeguards ~~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~~."

6. **Rec. (17)**

We refer to our comment regarding Article 11a.

7. **Rec. (17a)**

We welcome the fact that Recital 17a clarifies that the identifier can also be sector-specific. However, our main concerns regarding the establishment of a persistent unique identifier remain. While we do see the need for a mechanism to uniquely identify users in cross-border situations, we see the risks arising from a unique and persistent identifier available to both the public and private sector for the fundamental rights of natural persons. Currently we do not see sufficient safeguards to mitigate those risks.
Please see also our comments regarding Articles 3 (55a) and 11a.

Specifically, we see the following issues:

- The introduction of a "mechanism that allows for the use of relying party specific identifiers in cases when the use of a unique and persistent identifier is not required by national or Union law": from our understanding, this would mean to turn away from the initial approach by COM to allow the use of a unique identifier provided by the Wallet only if its use is required by law. We cannot support such a broadening of the use of identifiers as this would mean to take away one of its most fundamental safeguards.
- While the Recital states that users have to be protected against misuse, profiling and tracking, there are no specifications in the Presidency (PCY) compromise proposal what measures that would imply and which specific safeguards the PCY has in mind.
- Lastly, we have difficulties to understand what the PCY means by "administrative practice". From our understanding, administrative practice alone cannot legitimate the processing of a unique and persistent identifier, as Article 6 (3) GDPR requires provisions laid down in Union or national law.

8. Rec. (20)

The GDPR requirements for data transfers to third countries have to be met. In our view, the wording "considered" does not sufficiently reflect that these are binding legal prerequisites. The provision should therefore read as follows:

"When setting out 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, compliance with the relevant provisions in the Directive XXXX/XXXX, (NIS2 Directive) and Regulation (EU) 2016/679 should ~~also~~ be ~~considered~~ ensured, as well as the use of trusted lists as essential elements to build trust. ".

9. Rec. (24)

We suggest the following changes:

"(…) In order to ensure that the data using a qualified electronic registered delivery service is delivered to the correct addressee, as well as authenticity and non-repudiation of the sender, qualified electronic registered delivery services should ensure with assurance level "high" ~~full certainty~~ the identification of the sender as well as of the addressee ~~addressee while a high level of confidence would suffice as regard to the identification of the sender.~~"

10. Rec. (28)

Self-regulatory codes of conduct can be a meaningful tool, but only if they are uniformly designed and if they are used by providers on a mandatory basis. This requires that a certain body, e. g. the COM, takes the lead regarding the development. We would therefore be interested to learn how the COM envisions the development process.

11. Rec. (29)

In the second sentence, we suggest changes with view to the GDPR terminology. The reason behind this is that the authenticity of personal data and attributes is crucial for the secure authentication of citizens. However, in order to ensure convenience and personal data protection the European Identity Wallet should also technically prevent unauthorized copying of data, even if the authenticity of data is preserved. This is especially important for e.g. biometric data, cf. (11).

The provision should therefore read as follows:

"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 the protection of personal data ~~protection~~ including data minimisation ~~of processing of personal data~~. The European Digital Identity Wallet should also technically prevent unauthorized duplication of personal data and attributes."

12. Rec. (32)

We would like to point out that the wording "justified concerns" in the penultimate sentence is too vague and thus leaves all options open to the providers of web browsers to not display the website certificates as before. We suggest deleting this sentence or at least defining the term "justified concerns".

13. Rec. (33)

With regards to this recital but also as a general comment in the context of "archiving" we suggest to use the wider term "data" Instead of "electronic document". "Document" is linked to document formats e.g. PDF, but data contains images, research data etc. too, which can be used by trust services. We would like to make the following suggestion:

"Many Member States have introduced national requirements for services providing secure and trustworthy digital archiving in order to allow for the long term conservation of electronic ~~documents~~ data and associated trust services. (…) When required, these provisions should allow for the conserved electronic ~~documents~~ data to be ported on different media or formats for the purpose of extending their durability and legibility beyond the technological validity period, while minimising loss and alteration to the greatest extent possible. When electronic ~~documents~~ data submitted to the digital archiving service contain one or more qualified electronic signatures or qualified electronic seals, the service should use procedures and technologies capable of extending their trustworthiness for the conservation period of such documents, ~~possibly~~ relying on the use of other qualified electronic trust services established by this Regulation."

14. Rec. (34)

The current proposal emphasizes that electronic ledgers should be characterised by their sequential chronological ordering as it prevents double-spending. However, the chronological ordering does not help in covering those security aspects that are crucial for most of the intended applications (i.e. the data in the ledger are authentic, time-stamps are reliable). Therefore, we are convinced that the ledger definitions in this proposal are insufficient for establishing trust on such a level as would be expected from eIDAS.

Our comments in detail (cf. also recital (35), Art. 45h and Art. 45i):

- Sentence 1 ("Electronic ledgers… chronological ordering."): see Art. 3(53) for comments on "sequence" and "chronological ordering".
- Sentence 3+4 ("Electronic ledgers… public services."): These sentences are statements enumerating potential use cases of electronic ledgers without providing any reliable justification. Such statements are well-known from DLT/blockchain sales pitches, but should not be part of a recital of an EU regulation. Moreover, for all of these use cases, it would be absolutely crucial that only authentic data is stored in the electronic ledger. However, electronic ledgers as defined in the current draft of the regulation do not provide authenticity, only integrity and chronological ordering.
- Sentence 5 ("Qualified electronic…in the ledger"): The way the qualified electronic ledgers are characterized here seems to be identical to the (non-qualified) electronic ledgers as defined in the first sentence.
- We suggest (cf. Art. 45i) that qualified electronic ledgers must also guarantee that the stored data is authentic. This would be a clear distinction between qualified and non-qualified ledgers.
- See Art. 45h, 2. for a comment on "unique".
- Sentence 7 ("Namely, neither... different parties"): We disagree with this generalisation. Qualified electronic time stamps could also be used to establish a transaction history, thus helping to detect/avoid double-spending, though by different methods. The last sentence ("The process… or distributed)") is in principle valid although it is never referred to in the regulation and as such seems dispensable.

15. Rec. (35)

We suggest to delete this recital. The current proposal explicitly excludes from this regulation any verification of the authenticity of the ledger data and/or its sources. This is not acceptable since it renders the data absolutely unreliable -- in contrast to the otherwise high standards on trust in the eIDAS regulation.
We recommend to rather delete any reference to electronic ledgers from this regulation than to allow such a deviation from eIDAS standards.
(Cf. recital (34), Art. 45h and Art. 45i.)

16. Art. 2 (3)

In Article 2 (3) eIDAS Regulation, it is still important for us that the already existing exceptions regarding form in contract law and other legal and procedural requirements can be retained unchanged. The current wording could be misunderstood to mean only sector-specific requirements regarding form and not, as intended, also general formal requirements (see recital 19). We therefore prefer the wording as contained in the first compromise proposal of the FRA PCY.

17. Art. 3 (2)

The usage of an "electronic identification means" should be restricted to the online authentication only. In the "offline" case different requirements and a different type of authentication can take place (e.g. considering an image of the person). We propose to delete "or offline".

18. Art. 3 (5a)

We understand the definition to include relying parties. If this is the case, then the use of the term "user" in Art. 45d must be reconsidered, as it would not make sense for relying parties to request the trust service providers to check the attributes against the authentic source. In Art. 45, this only makes sense if "user" is the principal who wants to use the attributes.

19. Art. 3 (16)

Firstly, an undefined service cannot be audited and approved if there are no rules governing it (how should regulators monitor an undefined trust service?). Secondly, validation should be related to the customer product, i.e. signatures, timestamps, etc., the validation of certificates has no use of its own besides this. Thirdly, the management of devices" is not the service offered and completely unclear to the customer. These are signing or sealing services, which are covered under (b). Lastly, for registered mail delivery services, validation of all parties is a core functionality of the service itself, validation alone is not possible, covered under (gab).
Therefore, we propose the following changes:

"'trust service' means an electronic service normally provided for remuneration which consists of:
(a) the issuing of certificates for electronic signatures, of certificates for electronic seals, of certificates for website authentication ~~or of certificates for the provision of other trust services~~ or electronic attestations of attributes; or
~~(aa) the validation of certificates for electronic signatures, of certificates for electronic seals, of certificates for website authentication or of certificates for the provision of other trust services;~~
(b) the creation of electronic signatures and or of electronic seals; or
(c) ~~the validation of electronic signatures and or of electronic seals;~~ the creation of electronic timestamps ; or
(d) the preservation of electronic signatures and of electronic seals ~~of certificates for electronic signatures or of certificates for electronic seals~~ ; or
(e) ~~the management of remote qualified electronic signature and seal creation devices or of remote qualified electronic seal creation devices;~~ the validation of electronic signatures, of electronic seals, of websites, of electronic timestamps or of electronic attestations of attributes; or
(f) ~~the issuing of electronic attestations of attributes~~ the provision of electronic registered delivery services; or
~~(fa) the validation of electronic attestation of attributes;~~
(g) ~~the creation of electronic timestamps ;~~ the electronic archiving of electronic documents; or
(ga) the validation of electronic timestamps; or
(gb) the provision of electronic registered delivery services; or

(gc) the validation of electronic registered delivery services;

(h) ~~the electronic archiving of electronic documents; or~~

(i) the recording of electronic data into an electronic ledger ; or

(j) ~~the recording of electronic data into an electronic ledger ;~~ any combination of the above services'

20. Art. 3 (42)

The definition is not congruent with Art. 6a par. 3b.

What does to create mean in this context? Does this mean that a wallet provider must also be a trust service provider?

21. Art. 3 (47)

We suggest the following changes:

"electronic archiving' means a service ensuring the receipt, storage, retrieval and deletion of electronic documents in order to ~~guarantee~~ preserve their durability and legibility ~~as well as to preserve their integrity and origin throughout the conservation period~~ throughout the retention period. It can be combined with a preservation service in order to preserve the authenticity, integrity and proof of existence of the data using digital signature techniques;

22. Art. 3 (50)

We suggest the following changes:

"'strong user authentication' means an authentication based on the use of ~~two or more elements categorised as~~ at least two authentication factors of different categories: user knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way to protect the confidentiality of the authentication data;"

23. Art. 3 (53)

We suggest to delete any reference to electronic ledgers (cf. recitals (34), (35), Art. 45h, Art 45i).

If not, we propose the following definition:

"'electronic ledger' means a collection of electronic data records, which ensures their integrity and provides an electronic time stamp for each data record it contains. These time stamps may be realised through a sequential chronological ordering."

Rationale:

- "sequence": Why should it not be allowed that data is stored in some arbitrary way (thus respecting technology neutrality)? A chronological ordering can be established by other means if needed (see below).
- "accuracy of chronological ordering": If the requirement that data be stored in a "sequence" is replaced by a (possibly non-sequential) "collection"—as we have just suggested for reasons of technology neutrality—then a chronological ordering is not immediately visible. Therefore, each data record would need to carry some sort of time stamp in order to retrieve the "chronological ordering" whenever needed. However, a sequential chronological ordering is superfluous in establishing trust (which is the main focus of eIDAS). It should therefore not be part of the definition (i.e. of the first sentence). This is why we suggest to move it to the second (optional) sentence. Note that our proposal would still cover the case that data is stored in a chronologically ordered sequence (like a blockchain), but would also allow a wider range of data structures.
- Note further that our proposal to introduce a time stamp in each data record can easily be adjusted to require qualified electronic time stamps for qualified electronic ledgers (cf. Art. 45i).

24. Art. 3 (55a)

According to the PCY's approach, the identifier does not necessarily need to consist of a single personal identification number. Is our understanding correct that the current "data set" as set out in the Annex to Implementing Regulation 2015/1501 would be a unique and persistent identifier within the meaning of this definition?
In any case, it should be clarified that the requirements of the eIDAS Regulation do not differ from the above mentioned Implementing Regulation that requires the identifier to be "as persistent as possible in time". It is not evident that the Wallet only works with a persistent as opposed to a persistent as possible identifier. Also a unique identifier which is as persistent as possible in time allows for an identity matching based on the remaining attributes in the PID set.

Furthermore, the obligation to include a persistent identifier should be deleted due to data protection risks as well as from the point of view of investment protection. For Germany, the obligation to introduce a persistent identifier would raise a number of constitutional questions. The extension of the eIDAS Regulation to the private sector as well as the link with electronic attestations of attributes entail particular data privacy risks. A persistent identifier makes it possible to link an individual's activities to public authorities, private online platforms and companies and link identity data with possibly sensitive data from electronic attestations of attributes. We fear that online platforms would use the persistent identifier for more effective advertising profiling. This would jeopardize trust in the Wallet as a whole. Furthermore, the introduction of a mandatory persistent identifier would require legal and technical adaptions to all notified eID schemes that do not contain a persistent identifier, but an identifier that is as persistent as possible in accordance with the aforementioned Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015.

Therefore, we suggest the following changes:

"'unique and persistent identifier' means an identifier which may consist of either single or multiple national or sectoral identification data, is associated with a single user within a given system and as persistent as possible in time;"

Please also see our comments regarding Article 11a.

25. Artikel 5 1.

The former Art. 5 1. should be reinstated and should refer to the General Data Protection Regulation. We propose the following amendment:

„Processing of personal data falling within the scope of this regulation shall be carried out in accordance with Regulation (EU) 2016/679 and Directive 2002/58/EC, where relevant."

26. Art. 6a 3. (a)

It needs to be clarified what is meant by "presentation" in contrast to an authentication. In our view it is further necessary to submit data through an authenticated channel in each case. Therefore, the provision should read:

"securely request, select, combine, store, delete and ~~present~~ submit electronic attestation of attributes and person identification data through an authenticated channel to relying parties, including to authenticate online and offline in order to use online public and private services, while ensuring that selective disclosure of data is possible; "

27. Art. 6a 3. (ab)

This paragraph should be reinstated as electronic identification and authentication is an important feature. Furthermore, we consider it important to only restrict this to the usage of notified eID means. This would ensure the reusability of existing developments by MS, as well as providing a base line of requirements and an established and proven procedure for establishing trust in the security of these means.

28. Art. 6a 4. (a) (1)

"person identification data" should be deleted as the issuance of person identification data to the wallet depends on the national implementation and therefore should not be restricted to one "common interface".

29. Art. 6a 4. (a) (3)

It is still unclear what is exactly meant by "presentation". Furthermore, it is important to have a common interface for authentication of the user to the relying party. Therefore, we suggest the following wording:

"for the ~~presentation~~ authentication to relying parties and submission of person identification data or electronic attestation of attributes online and, where technically feasible, ~~also offline~~;"

30. Art. 6a 4. (b)

We kindly ask the PCY to explain what services it has in mind for whose provision information on the use of attributes would be strictly necessary. When users request a service, practice shows that they will often lack an overview and understanding of which of their data they would have to disclose by consequence, as well as the ability to assess whether the disclosure of such data is really necessary.

In addition, practice shows that providers already tend to interpret the "(strict) necessity" of processing data broadly. We believe that users should be protected from such scenarios when using their Wallet, and we do not see that this would add a lot of value to users that could outweighs the risks. Lastly, "strictly necessary" (unlike "necessary") also seems to be an unknown term in existing data protection legislation and could lead to legal uncertainty. Therefore, we ask for deletion of the last half-sentence in brackets ("beyond what is strictly necessary for provision of a service requested by the user").

31. Art. 6a 4. (d)

As it is important for the relying party to authenticate the user and not "only" receive signed data, this paragraph should be reinstated.

32. Art. 6a 4. (e)

We refer to our comment on rec. (55) and propose the following change:

"ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and as persistently as possible in time represent the natural person, or legal person or the natural person representing the natural or legal person, who is associated with it the wallet;"

33. Art. 6a 6a.

As some member states already have components in their eID schemes that may be reused within a wallet in order to optimize the coexistence, "additional" should be removed.

34. Art. 6a 7.

It is not clear to us why the text was changed to "users" as it seems difficult to ensure that more than one user is in full control of the Wallet. Therefore, we suggest to delete “unless the user gives expressly requested consent to it”.

Also, we have concerns regarding the provision that a user can demand further data processing. Please see also our comments regarding para. 4 (b).

We are furthermore in favour of the requirement for issuers of the Wallet to keep personal data relating to Wallets also physically separate from their other data. This is a fundamental safeguard that we consider to be necessary for an official digital identity infrastructure not only for reasons of personal data protection, but also for security reasons. We suggest the following amendment:

“Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate (…)”

35. Art. 6a 11.

The (member state specific) on-boarding should fulfil the requirements laid down in Implementing Decision 2015/1502 related to level of assurance "high". This also includes the combination of different proofs, means and technologies. This paragraph should either be removed, or the suggested wording should be added:

“(…)This implementing act shall ensure the fulfilment of the requirements laid down in Implementing Decision 2015/1502 of 8 September 2015 related to level of assurance high and shall be adopted in accordance with the examination procedure referred to in Article 48(2).”

36. Art. 6b 1a.

We suggest deletion of this paragraph as we are against eliminating the registration obligation for fully offline use scenarios. Please see our comment regarding Recital 8a.

We are particularly concerned about paragraph 1a (ii). According to Article 5 (1) (c) and (e) GDPR, personal data must always be deleted or anonymised once the purpose of their processing has been achieved. The restriction in paragraph 1a (ii) is thus without any additional effect and thus does not provide an efficient safeguard.

37. Art. 6b 3.

In our view, it is not sufficient to authenticate "data", but it is necessary to authenticate the user of the wallet. We suggest the following wording:

“Relying parties shall be responsible for carrying out the procedure for authenticating the user and **validating** person identification data and electronic attestation of at tributes originating from European Digital Identity Wallets.”

38. Art. 6c 1.

This paragraph should be adjusted: In our view, the assessment should still be carried out in a peer review and not solely base on certification. Following the Building Block approach, a to be peer reviewed wallet could be composed of different modules/building blocks that are certified according to a fixed scheme. If these components have been peer reviewed once, they could be easily reused without being assessed deeply again. This would make the peer reviews much faster by maintaining their harmonizing effect.

39. Art. 6 db 1. and 2.

An exception for the health care sector must be added to Article 6 (db) No. 1. We propose the following wording:

"This does not apply to public sector bodies in the health care sector."

Furthermore, such an exception must also be added to Article 6 (db) No. 2. We propose the following wording:

"This does not apply to private sector bodies in the health care sector."

Rationale:
To avoid potentially significant costs, these provisions may not be mandatory for Member State health systems. Healthcare-specific identification and authentication means already exist in Member States with high trust levels (specifically assessed for sufficient trust levels for access to highly sensitive personal health data). If healthcare providers in Member States were required to accept the European Digital Identity Wallet, the certification requirements regarding the required trust level would be even higher than for a (general) trust level "high" for (most) other use cases that do not involve access to highly sensitive personal health data.

This comment does not apply to health-related attestations or certificates like the EU Digital Covid Certificate (EU-DCC) that are explicitly meant to be used for specific but general purposes and use cases mostly outside the health care domain.

40. Art. 6 db 4.

We refer to our comment regarding recital (28): Self-regulatory codes of conduct can be a meaningful tool, but only if they are uniformly designed and if they are used by providers on a mandatory basis. This requires that a certain body, e. g. the COM, takes the lead regarding the development. We would therefore be interested to learn how the COM envisions the development process.

41. Art. 11a 1.

We refer to our comment regarding recital 17a.

42. Art. 11a 2.

Please also see our comments regarding Article 3 (55a): As under the current eIDAS legislation, it should remain left to the Member States to decide whether or not to use a persistent identifier. Hence, the current scheme should be maintained (as regulated by Implementing Decision 2015/1501 of 8 September 2015), see drafting suggestion.
Regarding the notion of "administrative practice", please see also our comment regarding Recital 17a.
Therefore, we have the following drafting suggestion:

"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 accordance with the technical specifications for the purposes of cross-border identification and in conformity with Union and national law, to identify the user upon their request in those cases where identification of the user is required by law **~~or is in accordance with administrative practice~~**]."

43. Art. 12 4. (d)

From our point of view, the Digital identity Wallet alone is not an eID means, but only in combination with references to appropriate eID means.
With regard to the rationale of the suggested change in wording, please see the comment on Article 11a. We suggest the following changes:

"'a reference to a minimum set of person identification data necessary to uniquely and as persistently as possible in time represent a natural **person,** ~~or~~ legal person **or a natural person representing natural or legal persons**;'"

44. Art 12 6. (ca)

The application of Article 6(1)(f) of the Regulation XXX/XXXX [DMA] for granting access to security components for the issuing and operation of (European) electronic identification schemes and EUDI-Wallets must be explicitly specified in the (eIDAS) regulation to provide planning security for (European) service providers and protect them from any risk that gatekeepers would make a legal claim that the access to any security component using them for ID means might not fall under the scope of the DMA.
If this certainty cannot not be achieved in advance of establishing a new service on the basis of the security components, it will be unlikely that European providers for electronic identification schemes will take the risk for investments for providing these services with the consequence that high assurance and trust levels can only be provided by the gatekeepers themselves. We therefore suggest to replace this paragraph with the following provision:

“In cases of Article 6(1)(f) of the Regulation XXX/XXXX [DMA], gatekeepers must allow issuers of electronic identification schemes notified pursuant to Article 9(1) access to hardware or software features of the device to enable security functions for electronic identification means notified pursuant to Article 9(1) and the European Digital Identity Wallet as well as their use. Access must include administrative access to security components with the possibility for the issuer of electronic identification schemes to install applications on the security components. Article 7(1) of the Regulation XXX/XXXX [DMA] applies accordingly to the assurance of access.“

45. Art. 12a 2.

Similar to our comment related to the certification of wallets, this paragraph should be adjusted as well in order to implement a peer review also in this case.

46. Art. 19a 1. (b)

The insertion of "affected individuals" leads to a (further) overlap with Articles 33 and 34 GDPR as far as personal data are concerned.
Rationale:

- Obligation to notify to supervisory authority already results from Art. 33 GDPR in the regulated case, however with 72h and not 24h deadline as provided for here.

- The GDPR also regulates the contents to be reported and a documentation obligation, which is missing here.
- Obligation to notify data subjects already results from Art. 34 GDPR; however, "affected individuals" are probably not synonymous with data subjects within the meaning of the GDPR. It is overall questionable whether obligations should apply in parallel; risk of legal uncertainty also for providers.

Please explain how the PCY sees the relationship to the notification and reporting obligations of the GDPR and why such a regulation deviating from the GDPR is proposed here.

47. Art. 24 1. (a)

If the Wallet is notified or relies on a notified eID mean, it does not need to be mentioned separately. Otherwise, it should not be sufficient for issuance of a qualified certificate. Therefore, we suggest the following deletion:

“by means of ~~the European Digital Identity Wallet or~~ a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance level ‘high’;”

48. Art. 24 1. (c)

In order to clarify the requirements that are applicable, the concept of the levels of assurance should also be reused here. Consequently, also the corresponding requirements should be valid. Therefore, "a high level of confidence" should be changed to "a high level of assurance".

49. Art. 45d 1.

We would like to know for what qualified providers are needed? Is the authentic source not sufficient to verify the attributes?

50. Art. 45g 2.

We would have the following drafting suggestion:

“Electronic documents stored using a qualified electronic archiving "proof of existence ~~and of their origin~~ for the duration of the conservation period, if ~~by~~ the qualified trust service provider can provide the proofs of integrity, authenticity and existence, producing by itself or by using a preservation service.”

51. Art. 45ga 1. (b)

We suggest the following changes:

“They use preservation procedures and technologies ~~capable of extending the durability and legibility of the electronic document beyond the technological validity period and at least throughout the legal or contractual conservation period, while maintaining their integrity and their origin~~ that guarantee the integrity authenticity and proof of existence of the electronic documents, whether they are signed or not, for the duration of the preservation period as a by the qualified trust service providers;”

52. Art. 45ga 1. (c)

We would have the following drafting suggestion

“They ensure that the ~~electronic documents are~~ data is ~~stored~~ archived in such a way that ~~they are~~ it is safeguarded against loss and alteration, except for changes concerning ~~their~~ its medium or electronic format and further on, is negotiable and independent of a specific storage medium;”

53. Art. 45ga 1. (d)

The eIDAS-Regulation is not the right place for technical requirements (here provision of a report). These technical requirements are to be written down in the standards according Article 45ga, 2., referenced by means of implementing acts.

If the archived data are signed the proposal is in contradiction to Art. 34 and 40 eIDAS which require the preservation of the (qualified) electronic signature resp. signed data. Therefore, this point is not general enough and not technical neutral and should be changed

"They shall allow authorised relying parties to receive a report in an automated manner ~~that confirms that an electronic document retrieved from a qualified electronic archive enjoys the presumption of integrity of the data from the moment of archiving to the moment of retrieval. This report shall be provided in a reliable and efficient way, which report is reliable, efficient and it shall bears the advanced qualified electronic signature or advanced qualified electronic seal of the provider of the qualified electronic archiving service~~, further on the archived data only or the archived data with its preservation evidences or with validation report(s) produced by the archiving or preservation trust service provider, which demonstrates that one or more archiving-preservation goals are met for a given archived object (e.g. integrity, authenticity, proof of existence of digital data at a given time, validity status of the electronic signatures and seals, etc.);"

54. Art. 45ga 1. (e)

We kindly ask the PCY to reinstate this paragraph.

55. Section 11

We strongly recommend to delete any reference to (qualified) electronic ledgers from the regulation for the following reasons:

- It does not become clear which role the ledgers are supposed to play in the eIDAS context. The use cases sketched in recital (34) are vague and only repeat, without any profound justification, what is being advertised by the DLT community.
- The definitions in Art. 3 (53) and (53a) are not sufficiently mature. Apparently, there is no consensus about what a ledger really is, what it will be used for, and which (security) properties it hence must provide. In particular, not requiring that ledgers guarantee authenticity makes them useless.
- To us it seems that the only reason for introducing electronic ledgers is the establishment of DLT in the eIDAS context. This is an ill-conceived approach, lacks a profound motivation and contradicts technology neutrality.

Alternatively: see drafting suggestions below.

56. Art. 45h 2.

We suggest deletion and alternatively the following changes:

"Data records contained in ~~a qualified~~ an electronic ledger shall enjoy the presumption of their ~~unique and accurate sequential chronological ordering and of their~~ integrity.

Data records contained in a qualified electronic ledger shall enjoy the presumption of their integrity and authenticity. They shall further enjoy the presumption of the accuracy of the date and the time indicated by their qualified electronic time stamps as laid down in Article 41."

Rationale:

- "To us, it is unclear what a "unique sequential chronological ordering is supposed to be.
- "accurate sequential chronological ordering": The definition of "electronic ledger" does not contain any guarantees about the authenticity of the time stamp/chronological ordering. Therefore, it must not enjoy the presumption of accurate chronological ordering.

(Note: Our drafting suggestion is based on our proposed changes in Art. 45i below. If those changes are not accepted then the drafting suggestion for Art. 45h point 3 would have to be reworked)

57. Art. 45i 1. (b)

We strongly suggest to be more precise about what it means to "establish the origin of data records":

Data in a qualified electronic ledger must be guaranteed to be authentic to be of any practical use in the context of the regulation. Since ledgers cannot technically verify the authenticity themselves, this task has to be performed by a qualified trust service provider. The TSP should then sign the data with a QES, thus providing a proof of authenticity to be included in the ledger.

Only with these changes can the qualified electronic ledger enjoy the presumption of authenticity (cf. 45h, 3).

- “chronological ordering”: see our comment on Art. 3 (53)
  Ordinary electronic time stamps – e.g., such as can be derived from a sequential chronological ordering – do not provide a sufficient level of trust in the correctness of the alleged time and date. Although this may be enough for ordinary electronic ledgers, qualified electronic ledgers should incorporate qualified electronic time stamps.
  Note: Only with a qualified time stamp can the ledger enjoy the presumption of accuracy of date and time (cf. 45h, 3).

We suggest the following changes:

> “they ~~establish the origin of data records in the ledger;~~ contain for each data record a proof provided by a qualified trust service provider that the trust service provider has verified the authenticity of the data and its source;”

58. Art. 45i 1. (c)

Based on the aforementioned rationale, we suggest the following drafting:

“they ensure the ~~unique sequential chronological ordering of data records in the ledger;~~ accuracy of date and time of each data record in the ledger by means of qualified electronic time stamps;"

59. Annex I (x) und Annex III (x)

As other MS, we think that these amendments have to be revised.

60. Annex VI

The list of attributes in Annex VI is too general and abstract.

The last sentence in recital 30 "Specific attributes falling into these categories should be agreed upon Member States" should be supplemented by the definition of these attributes before the regulation enters into force. Any other approach contradicts the harmonization idea of the Regulation.

Council of the European Union
General Secretariat

Brussels, 20 September 2022

WK 12312/2022 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 : DE comments (doc. 11713/22)

Delegations will find in the annex the DE comments on European Digital Identity.