EUROSMART
The Voice of the Digital Security Industry

European digital identity framework – Towards the interinstitutional discussions

Eurosmart's comments on the European Parliament position

On March 15, the European Parliament approved the decision to enter interinstitutional negotiations. Ahead of the Trilogues meetings to starts on March 21, and as a complement to Eurosmart's comments on the Council's General Approach, Eurosmart shares its policy and technical position to initiate an active debate between the co-legislators.

The European Digital Security industry is pleased that the legislative process is on good tracks. The current negotiating mandate of the industry committee (ITRE) of the European Parliament provides essential elements for the concreate implementation of the European digital identity framework a real; however, some improvements are still necessary to address the concerns shared between different stakeholders represented by Eurosmart.

Article 6a

European Digital Identity Wallet

ITRE report		Eurosmart comments	Eurosmart's recommendation
1. For the purpose of ensuring that all natural and legal persons in the Union have secure, ***reliable,*** trusted and seamless access to cross-border public and private services, ***while having full control over their data,*** each Member State shall issue ***at least one*** European Digital Identity Wallet ***by … [*** ***18*** months after the date of entry into force of ***this amending*** Regulation]	Positive	**Mandatory issuance of wallet proposed 18 months after the entry into force.** Eurosmart supports this ambitious planning which will ensure a quick uptake and deployment of the Wallet.	Eurosmart recommends maintaining this provision the trilogue discussions.
2. European Digital Identity Wallets shall be issued ***and managed in any of the following ways***: (a) ***directly*** by a Member State; (b) under a mandate from a Member State; (c) independently ***from a Member State*** but recognised by ***that*** ~~a~~ Member State***;***	Positive	**The proposal of QTSP has been withdrawn. The wallet shall then be recognized by that Member State.** Eurosmart warmly welcomes that the European Parliament has maintained the third option, and in particular the control by the Member States. In that case, wallet issuer shall be recognised by that Member State.	Eurosmart recommend maintaining this provision the trilogue discussions.
2a. The source code used for providing European Digital Identity Wallets	Negative	**Open source implementation for the Wallet**	Eurosmart recommends the withdrawal of this provision.

shall be open source, and shall be published for auditing and review.		This provision is unclear and raises several questions: - What is the meaning of open source? A clear definition is needed to support clear implementation of this provision. - What is the scope of the wallet at stake? A mobile App? Should the underlying OS also be considered? The hardware as well? Besides, security could be demonstrated with no open source implementation. Security certification has been used for decades to demonstrate security of non-open source implementation. In addition, critical assets such as sensitive cryptographic material requires a high level of security, for which open source may be detrimental by disclosing internal design and security countermeasures.	
3. European Digital Identity Wallets shall, ***in a user friendly manner,*** enable the user to: (a) securely request and obtain, store, select, combine and share, in a manner that is transparent to ~~and~~, traceable by ***and under the sole control of*** the user, the necessary ~~legal person~~ identification data ~~and electronic attestation of~~	Positive	**Online and Offline identification and authentication of the user** Eurosmart welcomes the position of the European Parliament whereby the wallet shall mandatorily support identification and authentication of the user online AND offline. Eurosmart highlights that both are needed so that the wallet could be used in any situation. Offline is very relevant when the user is willing to	Eurosmart recommends maintaining this provision the trilogue discussions.

~~attributes~~ to ***identify and*** authenticate ***the user*** online and offline in order to use online public and private services;		use its wallet during a physical transaction in a place where he doesn't have any network connection. The support of offline shall not be a possibility for the wallet but be mandatory in the same way as the support of online.	
3. European Digital Identity Wallets shall, ***in a user friendly manner,*** enable the user to: ***[…]*** ***(c) securely issue and revoke electronic attestation of attributes issued directly by the user;***	Neutral	**The wallet shall also issue attestations** What is meant by a wallet issuing and revoking an attestation is unclear. Does it imply that (1) the wallet issuer itself issues and guarantees an attestation or (2) the wallet itself issues and guarantees an attestation or (3) the wallet stores attestations received by an external TSP?	Eurosmart recommends the legislator to provide necessary additional clarifications to support implementation of the wallet.
3. European Digital Identity Wallets shall, ***in a user friendly manner,*** enable the user to: ***[…]*** ***(d) generate pseudonyms and store them encrypted and locally within it;***	Neutral	**The wallet shall also generate pseudonyms** Regarding the implementation perspective, pseudonym may also be dynamically generated and not stored. Indeed, implementation where pseudonym is stored are also possible.	Eurosmart recommends the co-legislators to amend the article as it follows: *"generate pseudonyms and**/or** store them encrypted and locally within it;"*
3. European Digital Identity Wallets shall, ***in a user friendly manner,*** enable the user to: ***[…]*** ***(e) securely authenticate a third person's European Digital***	Neutral	**New role for the wallet: "means of verification" wallet-to-wallet.** "Wallet-to-wallet" interaction is a very interesting concept which may be very useful to support the uptake and the deployment of the	

Identity Wallets or a connecting relying party, and receive and authenticate in a transparent and traceable manner the third party identity data and electronic attestation of attributes online and offline;		wallet. It will provide verification means to all users.	
3. European Digital Identity Wallets shall, ***in a user friendly manner,*** enable the user to: ***[…]*** ***(i) exercising their rights of data portability by switching to another European Digital Identity Wallet belonging to the same user.***	Neutral	**Users' right of data portability** Does the legislator intend to implement synchronisation between several devices/wallet – multiuser device belonging to the same user? - Option 1: is it an absolute right whereby the holder shall be able to exercise on its own at any time without third party supervision? - Option 2: A right that could only be exercised with third party supervision (e.g., PID issuer)	The meaning of "data portability" shall be specified and refer to article 20 of the Regulation (UE) 2016/679 (GPDR). According to Eurosmart, option 1 may raise security concerns: e.g., security of the target wallet is not controlled by the data issuer, binding between the wallet and the holder is not known. Eurosmart recommends only considering option 2: "under third party supervision".
4. ***European*** Digital Identity Wallets shall, in particular: (a) provide ~~a~~ common ~~interface~~ ***protocols and interfaces***: […] ***(6) for EDIW users or relying parties, when***	Negative	**Relying Party and wallet shall support ZKP for PID and attestations** The approach is not technologically neutral as it promotes a specific protocol. ZKP is one of the possible technologies that could be enabled to implement selective disclosure.	Eurosmart recommends the legislators to modify the provision as it follows: *"for EDIW users or relying parties, when available, to* ***~~perform a zero knowledge proof inferred from~~*** ***perform selective disclosure of*** *person identification data or electronic attestation of attributes"*

available, to perform a zero knowledge proof inferred from person identification data or electronic attestation of attributes;		The technological neutral terminology should rather be “Selective disclosure”.	This modification implies the withdrawal of recital 6c and the alteration of 3(5c) to provide a generic and “technology neutral” definition of “selective disclosure”: *Selective disclosure allows user to present a subset of attributes provided by the PID and/or (Q)EAAs.*
4. ***European*** Digital Identity Wallets shall, in particular: (a) provide ~~a~~ common ~~interface~~ ***protocols and interfaces***: ***[…]*** ***(7) for EDIW users to transfer and request reissuance of their own electronic attestation of attributes and configurations to another European Digital Identity Wallet belonging to the same user or a device controlled by the same user;***	Neutral	**Transfer and request reissuance of EAAs and configurations (not PID) to another wallet** Same concerns as for article 3 (i)	Same recommendations as for article 3 (i)
4. ***European*** Digital Identity Wallets shall, in particular: ***[…]***	Positive	**Concept of EAA bearing its own authorisation (disclosure policies)**	Eurosmart recommends maintaining this provision the trilogue discussions.

(c) ***in the case of electronic attestation of attributes with disclosure policies embedded, provide a mechanism to ensure that only the relying party or the EDIW user having the necessary electronic attestation of attribute giving permission access to it can access it;***		The Wallet shall verify it before disclosing the EAA. The wallet is to guarantee the user's security and data protection vis-à-vis the relying party.	
6a. ***The European Digital Identity Wallets shall ensure security-by-design. European Digital Identity Wallets shall provide the necessary state-of-the-art security functionalities, such us mechanisms to encrypt and store data in a way that is only accessible to and decryptable by the user and establish end-to-end encrypted exchanges with relying parties and other European Digital Identity Wallets. They shall offer resistance to skilled attackers, ensure the confidentiality, integrity and availability of their content, including person identification data and electronic attestation of attributes and request the secure, explicit and active user's confirmation of its operation.***	Positive	**End to end encrypted messages between the wallet and the RP/wallet - Requirement of availability of content on local storage - Request secure, explicit and active user's confirmation.** These provisions are fundamental to guarantee the wallet security.	Eurosmart recommends maintaining this provision the trilogue discussions.

Article 6c

Certification of the European Digital Identity Wallets

ITRE report		Eurosmart comments	Eurosmart's recommendation
1. European Digital Identity Wallets that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a ***of this Regulation*** ~~paragraphs 3, 4 and 5~~ in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. ***When relevant European cybersecurity certification schemes are available, the European Digital Identity Wallet, or parts thereof, shall be certified in accordance with such schemes.***	Negative	**Certification "High" is still not required** Eurosmart advocates for a security certification at level "high". This provision is necessary for the full implementation of article 4(6a).	Eurosmart recommends the legislator to modify the amendments to clearly mention the wallet certification at level "high". *Eurosmart has published a technical document focusing on this aspect*
3 The conformity of European Digital Identity Wallets with the requirements laid down in article 6a ***of this Regulation*** ~~paragraphs 3, 4 and 5~~ shall be certified by ~~accredited~~	Neutral	**On conformity assessments related to the Cybersecurity Act and GDPR approach**	Eurosmart recommends the co-legislators to specify the links and the requirements applicable for GDPR and Cybersecurity Act certifications processes.

~~public or private bodies designated by Member States~~ ***conformity assessment bodies in accordance with Article 60 of Regulation (EU) 2019/881 for cybersecurity requirements and by certification bodies in accordance with Article 43 of Regulation (EU) 2016/679 for personal data processing operations***.		Eurosmart raises concerns regarding the interpretation: The amendment is not referring to GDPR certification but only to GDPR certification bodies. How the article 6a requirements and in particular the requirements for personal data processing operations, would be concretely assessed? Moreover, GDPR certification remain on a voluntary basis. Moreover, the provision shall request the assessment by two types of assessments bodies.	

Article 45c

Requirements for qualified *electronic* attestation of attributes

ITRE report		Eurosmart comments	Eurosmart's recommendation
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. ***Only relying parties the user has shared this attribute with shall be able to link the revocation to those attributes.***	Negative	**This requirement hints at a particular implementation of revocation list** This requirement imposes to sort out the case where a qualified attestation is received directly from a user versus the case where it is transferred by another entity. In order to demonstrate that the qualified attestation has been truly received from the user, the relying party will have to collect supplemental information that may hamper privacy	Eurosmart recommends deleting this provision.

		(supplemental logs, session data, non-repudiable session data...). Besides, it seems this obligation rather applies to the provider of qualified attestation which is in charge of revoking the qualified attestation. It would entail that the latter will have to check the proofs submitted by the relying party to ensure the qualified attestation has been directly received from the user. This would contradicts with the key privacy requirement whereby the provider of qualified attestation shall not know where the qualified attestation is used after issuance (article 6a.4(b)).	

SECTION 11

Electronic ledgers

ITRE report		Eurosmart comments	Eurosmart’s recommendation
~~*Article 45h*~~ ~~**Legal effects of electronic ledgers**~~ ~~*Article 45i*~~ ~~**Requirements for qualified electronic ledgers**~~	Neutral	**Section 11 on Electronic ledgers deleted** This section as proposed by the European Commission provides a legal framework for such services.	Eurosmart recommends reintegrating this title during the trilogue discussions.