

# Digital Europe funding for identity: key principles

---

March 2022

The Digital Europe programme covers important projects in the field of digital identity. Thus, Digital Europe will fund the European Digital Identity Wallet prototype via procurement. The Programme will also support the development of large-scale pilot projects for the Wallet.<sup>1</sup>

Eurosmart would like to give key recommendations for the evaluation of the project proposals.

## Favour solutions relying on secure elements & CSA certification

Secure elements in smartphones and identity cards provide a safe place for identity data and cryptographic keys. Therefore, Wallets leveraging secure elements offer a very high level of resistance against cyber-attacks. This is even more the case if the hardware at stake has been certified using the EU Common Criteria (EUCC) certification scheme, the first EU-wide security certification scheme established under Regulation 2019/881 (Cybersecurity Act).

Without security, the implementation of the European Digital Identity Wallet cannot be successful. One large-scale cybersecurity attack is enough to hamper the trust users place in the Wallet and eventually discourage them from using it. Therefore, security should be at the heart of the Wallet prototype and Wallet pilot projects:

- Wallets relying on secure elements, either in the smartphone or the identity card, should be at the core of the Wallet prototype and Wallet pilots.
- Security certification using Cybersecurity Act (CSA) schemes, in particular EUCC certification of the eUICC<sup>2</sup> hardware, should be preferred.

## Take digital sovereignty into account

The Wallet prototype and the pilots are unique opportunities to develop an innovative European ecosystem further. Digital identity is closely linked to digital sovereignty. The data at stake relates to identity and sensitive information, such as financial data. It is only logical to ensure that private actors involved in the Wallet are entirely trustworthy. In Eurosmart's views, the European place of establishment and European control are adequate safeguards against a potential loss of sovereignty. Therefore, these parameters should be seriously considered during the evaluation process of both the

---

<sup>1</sup> The dedicated [call for proposals](#) opened on 22 February 2022.

<sup>2</sup> Embedded Universal Integrated Circuit Card.

tenderers and the pilot project proposals. In short, the European place of establishment and control should lead to bonus points for this evaluation.

Such an aspect is also relevant when it comes to the cloud. To a certain extent, Wallets are likely to rely on the cloud. Eurosmart believes that cloud providers should be established in Europe and controlled by European entities to avoid extra-territorial interference and ensure data could not be accessed by entities located in third countries. This precaution is crucial given the criticality of the information at stake. This is also the best way to guarantee compliance with privacy rules. Therefore, Eurosmart recommends giving bonus points to the tenderers and project proposals that put the emphasis on the European localisation and processing of data, as well as the protection of data from access from entities located in third countries.

Finally, Eurosmart believes that the European Commission should perform a security review of the submitted proposals, as provided by Article 12(3) of the Digital Europe Regulation.

## Rely on existing standards

Eurosmart has long been advocating for the use of existing standards for this future European Digital Identity Wallet. One standard stands out: ISO/IEC 18013-5 and its correlated ISO/IEC 23220 series of standards. These standards have the advantage of enabling the connection of different solutions. They are therefore well-suited for an agnostic approach. These standards allow for:

- (1) a variety of secure areas (eSE, eUICC, iSE, etc.) onboard the user device,
- (2) discretionary secure data storage,
- (3) user consent on selective disclosure of identification data/attributes/credentials,
- (4) interoperability over several mobile communication channels,
- (5) online as well as offline identification and authentication,
- (6) device provisioning with high-level interoperability interfaces.

Eurosmart underlines that an international standard can be endorsed through the regular procedure used by CCMC and CEN-CENELEC BT, whereby an international ISO/IEC standard can be transferred to a European Norm (EN).

Thus, Eurosmart strongly recommends including these standards in the references to guide Wallet tenderers. Likewise, pilot projects could rely on these standards.

In addition, CEN CENELEC/TC 224 is currently developing a gap analysis that identifies all the technical standards that could apply for the European Digital Identity Wallet(s) and the missing standards for which a New Work Item (NWI) would be necessary. Such work is highly valuable and can also be incorporated in future tender and pilot projects. For aspects relating to interface with trust services, Eurosmart recommends leveraging the work of ETSI TC ESI, even though their work does not cover all necessary elements. The gap analysis aforementioned has shown that ETSI's New Work Items do not address all the needed requirements/functionalities of European Digital Identity Wallet(s).

## About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

## Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, Fingerprint Cards, G+D Mobile Security, IDEMIA, IN GROUPE, Infineon Technologies, NXP Semiconductors, PayCert, Prove & Run, Qualcomm, Real Casa de la Moneda, Samsung, SGS, STMicroelectronics, Synopsys, Thales, Tiempo Secure, Trusted Objects, TrustCB, TrustSEC, WISEkey, Winbond, Xilinx**), laboratories (**BrightSight, CCLab, CEA-Leti, Jtsec, Red Alert Labs, Serma**), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster, Smart Payment Association, SPAC, Mobismart, Danish Biometrics**).

Eurosmart is a member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, GlobalPlatform, ISO, SIA, TCG, Trusted Connectivity Alliance and others.

**EUROSMART**  
The Voice of the Digital Security Industry



[www.eurosmart.com](http://www.eurosmart.com)



[@Eurosmart\\_EU](https://twitter.com/Eurosmart_EU)



[@Eurosmart](https://www.linkedin.com/company/eurosmart)

Square de Meeûs 35 | 1000 Brussels | Belgium  
Tel +32 2 895 36 56 | mail [Contact@eurosmart.com](mailto:Contact@eurosmart.com)