EUROSMART
The Voice of the Digital Security Industry

Low Security in the European Digital Identity Wallet:

An Unacceptable Risk for Citizens and Businesses

The European Commission pledges future EU digital Identity (EUDI) wallets that will provide a safe, reliable and private means of digital identification for everyone in Europe. The current technical and regulatory developments raise serious doubts about the security and protection of the personal data of citizens and businesses who will use this wallet. In recent proposal for implementing acts, the European Commission has chosen not to mandate strict and rigorous cybersecurity certification of the physical components that form the core of the wallet.

Without a stringent requirement to rigorously assess the hardware component's resistance to skilled attackers, there can be no assurance that the private keys stored in the wallet will remain secure from compromise or theft.

Private keys are pivotal in upholding EU citizens' fundamental right to privacy and in enforcing Article 8 of the EU Charter of Fundamental Rights.

> “ *The widespread use of EUDI wallets and their reach across EU citizens will undoubtedly motivate actors with bad intention to probe the robustness of wallet implementations. Where the confidentiality of the private key cannot be entrusted to the highest level of protection, it is reasonable to expect these actors will find a way to retrieve these private keys.*

Given the uncertainty regarding the level of security required at EU level for the development of national and interoperable electronic identity wallets, citizens and businesses that are using them will be exposed to serious and unacceptable risks.

The development of both political and technical requirements should be grounded on a comprehensive risk analysis. Furthermore, given the rapidly evolving nature of cyber threats, the digital security industry urges ENISA to incorporate the risks associated with EUDI wallets in its annual threat landscape report.

The threat exposure is expending with by the obligation of mutual recognition: a compromission of a single wallet design will lead to widespread exploited vulnerabilities and have systemic impact across all the Member States.

To contribute to this debate Eurosmart reminds the following risks:

Nation/State threats actors and terrorist threats

A state or terrorist organization will take the time and have the means to evaluate the security of each wallet design. The EUDI wallet will receive, via the institutional provider and/or Wallet provider personal identification data (PID) and Electronic attestation of attributes (EEA), such as digital travel credentials (DTC). If the private key of one single authentic wallet is extracted, then,

- With the retrieval of DTC from the legitimate wallet, and simple copy/paste of both the DTC and the private key onto a mobile device, **it would allow terrorists to infiltrate the EU using a counterfeit EUDI wallet**. Indeed, contingent on the strength of the matching method between the DTC that was presented remotely by an individual and the later authentication of this individual once on-site, the checking barrier can be bypassed if the authentication method involves the stolen private key (e.g. to sign an authentication proof)
- The terrorist can gain unauthorized access to restricted areas.
- The terrorist can manipulate authorities by providing false information under a genuine identity (e.g., bomb threats, false reports, ...).
-

This risk exposure is expected to align with a growing trend, as the EUDI Wallet and Digital Travel Credentials (DTC) are likely to be used for both transatlantic and non-EU travel. The EU-US Trade and Technology Council and pilots project have already been addressing the topic of transatlantic DTCs during a recent EU-US digital identity exercise mapping, and pilot projects are ongoing.

EU citizens victim of Impersonation attacks

With non-state-of-the-art security measures, the EUDI wallet could be vulnerable to different hacking methods allowing fraudulent digital identities to be obtained and potentially granting access to various services:

- Impersonation attacks can be unleashed by PID cloning. PID presentation is assumed to be always performed with Level of Assurance (LoA) high. PID attestations come along with a proof of possession and a proof of association as evidence of their binding to a PID subject and a wallet unit. But with a compromised wallet, the high security barriers for PID presentation (LoA high) can be bypassed through private key cloning, leading to large-scale digital identity misuse. An attacker using PID from someone else can generate a proof of possession by using the stolen private key; as well, an attacker can perform a holder authentication contributing to LoA high with the victim's private key while presenting victim's PID.
- Provisioning Interception can happen when authorization codes are intercepted during the provisioning process to fraudulently obtain attributes (PIDs, electronic attestations)

from the victim, enabling further misuse. When OpenID protocol is used for provisioning of PID or Electronic Attestation of Attributes (EAA) , the authorization code, even though Proof Key for Code Exchange mitigation is applied, can be intercepted by a rogue mobile application along with a secret (called *code verifier*) if the latter is not properly protected by the wallet.

Economical prejudice against citizens and businesses

Even when **Relying Parties** diligently perform all verifications on EEAs or PID presentation, including legitimate holder binding, they remain at the mercy of fraud as soon as the Wallet Secure Cryptographic Device (WSCD) protecting the binding keys is compromised.

- **Bank Account Opening fraud:** the fraudster opens a new bank account under a false identity and immediately benefit from the bank overdraft.
- **Bank Account Access:** The EUDI wallet could provide electronic identification and the provision of attestation of attributes to support the fulfilment of strong customer authentication. Clones of LoA high PIDs will allow access to victims' bank accounts and initiate fraudulent money transfers, as soon as PID presentation supersedes specific financial sector security verifications.
- **Attestation Provider Abuse:** criminals will obtain attestations in the victim's name and fully exploit the stolen identity.
- **Fraudulent Signatures:** criminals can sign contracts such as real estate transactions or use the stolen identity for authentication in various settings.
- **Stock market manipulation:** identity theft of key figures allows the dissemination of fake news that can have huge impact on stock markets.

Industrial and corporate espionage, supply chain attacks:

- **Access to Sensitive Information:** stolen identities will allow access to confidential businesses and governmental data. Typically, remote recruitment processes are becoming increasingly common. A company that is the victim of recruitment under a false identity would see its sensitive data sucked up in a matter of hours.
- **Supply chain infiltration:** impersonating a key intermediary in the supply chain, a fake supplier can manage to tamper with goods, to inject trojans, vulnerabilities, to replace components, to destroy sensitive goods, ...
- **Electronic ledgers compromission**: ledgers being increasingly considered for secure storage and mostly based on Proof of Authority for their consensus algorithm, they are directly exposed to impersonation of authorities.

Election and Opinion Manipulation:

- **Vote Manipulation:** compromission of the private key enables cast votes on behalf of the victim, whether they are a citizen or a Member of Parliament.

- **Fake Proxies for Elections:** Each stolen identity can be used to generate fraudulent election proxies.
- **Manipulation of public opinion and destabilization:** impersonation allows the dissemination of fake information, all the more if the victim is a public or influential figure.

Fake Mobile Driving Licenses (mDL):

- **Store a genuine mDL on a mobile device:** Illegally storing a real mobile driver's license in a wallet allows to drive without any valid license.

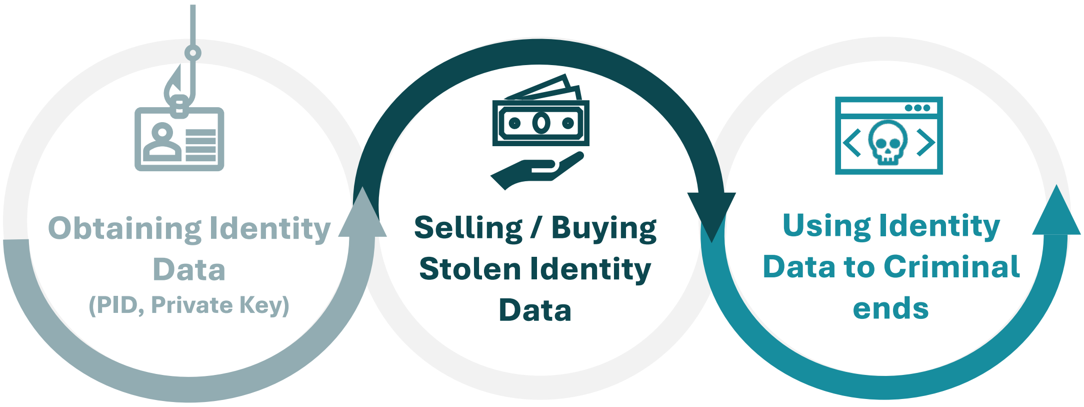
Digital scalability and Dark Web Exposure:

The purely digital nature of the wallet amplifies the risk exposure, and the existence of places like the Dark Web even more so:

- One of the primary consequences of EUDI wallet vulnerabilities is the likelihood of finding stolen identities, including PID and their respective private key(s) readily available on the dark web. These stolen identities could be exploited for a wide range of illegal activities.
- Wallet users would be forced to prove that the use of their PID is fraudulent. However, since private keys are supposed to be unique, expecting individuals to prove their innocence in the face of widespread identity fraud is quite unrealistic.

Fig. 1 – Stolen identity data lifecycle

Source: European Commission's Study on Online Identity theft and identity-related crime - 2022


Obtaining Identity Data
(PID, Private Key)
Selling / Buying Stolen Identity Data
Using Identity Data to Criminal ends

Attach vectors: data breaches, malware / illegal intrusion and interception
Social engineering: phishing, phone scams, business email compromised...

Exposure: Darkweb, surface web, peer-to-peer and communication channels (apps) using end-to-end encryption.

Examples: Fraud against individuals/companies
Libel/public defamation
Facilitation of terrorism
(S)extortion

How to mitigate the risks?

The EU has equipped itself with proper means to verify the level of security of EUDI wallets. Eurosmart urges the Commission to rely on what Europe has built:

> *Private keys of EU citizens must be protected with Hardware EUCC or SOGIS certified at EAL4+ AVA_VAN5 level*

Eurosmart industries have a long experience in delivering appropriate solutions, some of which being already available. Eurosmart industries are also confident to enable all envisaged solutions within schedule.

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.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com