Reg. No: 2023/51/I/ST6/02770; Principal Investigator: prof. dr hab. Mirosław Kutyłowski

IDanon:

Identity Wallet in a Hostile Environment: Privacy and Trust By-Design

Verifying the identity and/or credentials of participants in IT systems is one of the key components necessary for the secure operation of cyberspace. Additionally, identification processes should ensure that only the information disclosed is limited to the information necessary to allow the user to perform certain actions. This follows from the principle of data minimization, one of the basic computer security paradigms. It is also a requirement under current legislation, the GDPR Regulation of the European Parliament and the Council of Europe.

The minimization principle indicates the need for tools such as attribute certificates and tokens granting specific rights. In the first case, specific attributes of the user are disclosed (e.g., age of majority or professional entitlement) and not data identifying an individual. In the second case, attributes carrying specific entitlements are not even disclosed, but directly the entitlements themselves resulting from verification by the token issuer. An important type of token is the one-time token, now widely used as an effective replacement for unreliable CAPTCHA mechanisms.

The minimization principle applies not only to the end recipient of identification and authentication processes but also to the organization issuing the means for users to go through these processes. Mainly, when these organizations are centralized, it may lead to a situation where a significant amount of data about users' activities are gathered in one place. A successful attack on such an organization provides invaluable information for adversaries and poses a serious threat to public security.

The European eIDAS 2 Regulation, which is in the final stages of the legislative process, addresses these issues by introducing the idea of decentralizing the identity ecosystem. In this concept, an essential role is played by the European Identity Wallet - a device controlled by the identity holder, controlling the identification and authentication processes, particularly managing the attribute certificates received. Thus, the path from the source of attributes to their use by the holder is shortened.

The regulation only spells out the general idea, leaving free room for various implementations. Unfortunately, implementation faces many fundamental challenges. For this reason, current pilot programs focus on applications in simple, basic cases.

The European Identity Wallet, like many other cryptographic solutions, faces several critical issues that require urgent resolution. With such a large scale of applications, it must be taken into account that devices can be infected with hostile code, particularly from their manufacturer. This is particularly dangerous for black-box solutions. Devices may fail, and the supporting infrastructure may not be available. Finally, due to the lack of strong access control mechanisms, third parties can use the device for impersonation purposes.

The project aims to present solutions that make the identity ecosystem more resilient to these threats. One paradigm is to replace the wallet and supporting infrastructure with distributed systems so that the malfunction of individual components does not constitute a system collapse. At the same time, two goals will be met: data protection and user verifiability of processes. These mechanisms are to be realized in the cryptographic layer, to a high degree, independent of the hardware layer.

We will pay special attention to the issues of digital signatures and cryptographic token systems. In the latter case, we intend to realize the single-use tokens without relying on a central system for recording token usage. We achieve this by shifting responsibility to secure components distributed among users. A fundamental goal is also to liberalize the process of issuing tokens - so that the issuers can be the users themselves, not not just large organizations as is currently the case. Of course, a paradigm shift in operations requires building efficient cryptographic protocols with provable security, non-repudiation, and privacy properties. Last but not least, these solutions must be lightweight in the sense of communication and computational complexity, as well as transparent from the point of view of an average user not accepting too much "cryptographic magic".