FONDAZIONE BRUNO KESSLER MAGAZINE

# Towards a European digital identity

May 22, 2023

## FBK Center for Cybersecurity researchers Giada Sciarretta and Amir Sharif were invited to participate through the Department of Digital Transformation to collaborate on the eIDAS Expert Group table to develop the EUDI Wallet specification.

FBK-Cybersecurity provides solutions to address the challenges posed by emerging risks and to seize the opportunities generated by the development of digital identity management infrastructure, an enabling factor for the secure and privacy-compliant use of online services offered to citizens by companies and public institutions.

The development of digital identity management infrastructure brings numerous **benefits**, the most important of which are the following:

- providing users with a common identification and authentication experience for all those services that use the same digital identity management infrastructure;
- enabling
    - service providers to focus on developing new features and applications without having to deal with the user base and
    - digital identity infrastructure developers to focus on managing the life cycle of users allowing to optimize investments in terms of budget and skills for both service and digital identity managers.

Along with the benefits, digital identity management brings with it a number of risks such as:

- **insecurity** – an infrastructure vulnerability can have catastrophic consequences if exploited in an attack that allows, for example, the exfiltration of personal data that can later be used as a base for identity theft; and
- **lack of privacy** – the infrastructure's management of data must give utmost consideration to the privacy of users because such data, if not adequately protected, could be used for large-scale profiling activities supporting the mass surveillance model with highly negative consequences for people's fundamental rights and freedoms.

FBK Cybersecurity Center's objective and research activities

Therefore, it becomes critical to design, develop, and implement digital identity infrastructures in a way that ensures security and privacy. To this end, **FBK's Cybersecurity Center** develops methodologies applicable throughout the development cycle of digital identity management infrastructures supported by automated tools for the analysis and assessment of security and privacy risks. The use of automated tools makes it possible to quickly and traceably evaluate different alternatives from the conception of the infrastructure and then move on to screen different architectures and cryptographic protocols for data exchange until exhaustive security testing is performed on the infrastructure under production. All of this would be impossible without the automated component that also allows for precise and verifiable tracking of the design, development, implementation and configuration choices made to make the final infrastructure more transparent by simplifying audit processes by various stakeholders including experts appointed by citizen and consumer rights associations as well as national (such as ACN or **AgID**) or international (such as the **European Commission**) regulators.

Innovation at FBK’s Cybersecurity Center.

Confirmation of the relevance of the Center’s contributions comes from publications in international cybersecurity conferences and journals. The validation of the techniques developed by the Center is complemented by the numerous project activities of co-design and development of solutions for digital identity management with various entities including

- **Poligrafico e Zecca dello Stato (IPZS)** for the development of methodologies for the secure design of authentication infrastructures based on the electronic identity card Carta d?Identità Elettronica (CIE) 3.0 (such as the ?Entra con CIE? button to access Italian Public Administration services); and
- various public and private organizations within the European ?Large Scale Pilot EUDI Wallet? POTENTIAL project that aims to build the new European digital identity infrastructure in accordance with the new version of the **eIDAS 2.0**

For FBK’s Cybersecurity Center, there are two major **research and innovation challenges**, among the many posed by the secure development of digital identity infrastructure, that emerge as particularly important:

- in order to integrate authentication mechanisms for the secure use of sensitive services such as those for payments or health data management, a key pre-requisite is to minimize cyber risks in the identification phase (also called onboarding) during which it is verified that a user is really who he or she says he or she is and credentials are issued that will later be used in the authentication phase. Given the push to digitize many Public Administration processes (especially health care) as well as private ones (such as banking) accelerated by the COVID-19 pandemic, identification processes have also been digitized without the constraint of presence (e.g., it is possible to create a checking account without physically going to a bank branch). This transformation has led to the introduction of new attacks on remote identification processes that can lead to identity theft with potentially catastrophic consequences for the victim. For example, many processes use video fragments to compare the face of the person requesting digital identity creation with the image associated with the identity document submitted: modern image manipulation techniques including video (e.g., deep fakes) are able to virtually paste the face of the victim whose identity document has been stolen dynamically in such a way that it is difficult for image control algorithms or a human operator to find such manipulations.  The Center is developing techniques for detecting these types of threats and others that can undermine the ID process, providing a comprehensive classification of threats and related mitigations, while developing automated

techniques for risk assessment to help those developing these processes define the configuration of mitigations that will provide the desired level of security;
- in the short, medium and long term it will be necessary to integrate the infrastructure for the management of digital identity with the growing and increasingly complex ecosystem of services and applications offered by the **Italian and European Public Administration** in order to fully benefit from the advantages offered by **the digitalization of processes**. This needs to be done taking into account the different levels of maturity of the digital identity infrastructures in the various member states so as not to impose abrupt transitions on citizens. In other words, it will have to be understood how to manage the transition from infrastructures based on a centralized model currently available to the decentralized model based on **EUDI Wallet** envisaged by the new version of eIDAS (2.0). In particular, it will have to be understood whether the current infrastructures will have to be completely replaced or whether parts of it (e.g., those services for issuing certified attributes such as a driver's license) can be retained and integrated into the new ones.

**PERMALINK**

https://magazine.fbk.eu/en/news/towards-a-european-digital-identity/

**TAGS**

- #cybersecurity

**RELATED VIDEOS**

- https://www.youtube.com/watch?v=-sgJJv9kBao

**RELATED MEDIA**

- FBK-Cybersecurity: https://www.fbk.eu/en/cybersecurity/

**AUTHORS**

- Giancarlo Sciascia