ARIES: Reliable European Identity Ecosystem

by Nicolás Notario, Antonio Skarmeta, Jorge Bernal, José Luis Cánovas and Alberto Crespo

ARIES (ReliAble euRopean Identity EcoSystem) will provide secure privacy-preserving identity management, effectively reducing the risk of identity fraud and crime.

Personal data and individual identities are becoming increasingly vulnerable in the virtual world, which facilitates interaction between international stakeholders and the globalisation of crime. Public trust in online security is waning owing to the current lack of adequate solutions, including applied technologies and processes for trusted enrolment, identification and authentication processes. For example, most common authentication means are usernames and passwords, a solution that has been demonstrated to be vulnerable. Furthermore, there is a lack of a common EU wide concept of identity theft and room for improvement in the area of reporting mechanisms (especially across borders) [1] which costs companies, countries and citizens billions of Euros in fraud and theft. As acknowledged in the European Agenda on Security, 'cybercrime is an ever-growing threat to citizens' fundamental rights and to the economy, as well as to the development of a successful Digital Single Market' [2]

In this context, ARIES H2020 European research project [L1, L2] will enable secure, reliable and privacy-preserving identity management and derivation techniques, both to allow a secure user interaction with services and to prevent / reduce risks of identity theft and fraud crimes. ARIES ecosystem appears in the context of delivering a comprehensive framework and holistic approach of innovative technologies, improved processes and security features capable of enhancing the European eID ecosystem and achieving a tangible reduction in levels of identity theft, fraud and associated crimes.

ARIES ecosystem (see Figure 1) will empower its users with a mechanism (identity virtualisation process) allowing them to generate virtual identities, simultaneously linked to the citizens' biometrics and to existing digital or physical identities possessing a high level of identity assurance such as an eID or ePassport. These virtual identities can be stored and managed through a secure wallet usually installed in the citizens' smartphones. The usage of a convenient secure wallet to manage and present virtual identities will positively impact the usage of highly assured identities as it will avoid the usability issues and technological fragmentation (multiple standards) of physical identities and related technologies across Europe.

The ARIES ecosystem allows and encourages users to combine different virtual identities that have a high contextual value (e.g., national eID and bank information for an online transaction) into derived identities that minimises the data disclosed (e.g., there may be no need to disclose the sex of the person) and that can be reused in further interactions.

Cryptographic proofs for the identity enrolment, virtualisation and derivation processes can be stored, with the consent of users, in a secure vault that provides guarantees of integrity, confidentiality, auditability and compliance only accessible to law enforcement authorities when a cybersecurity incident occurs and when their assistance is required to help recover from an identity theft or loss [3].
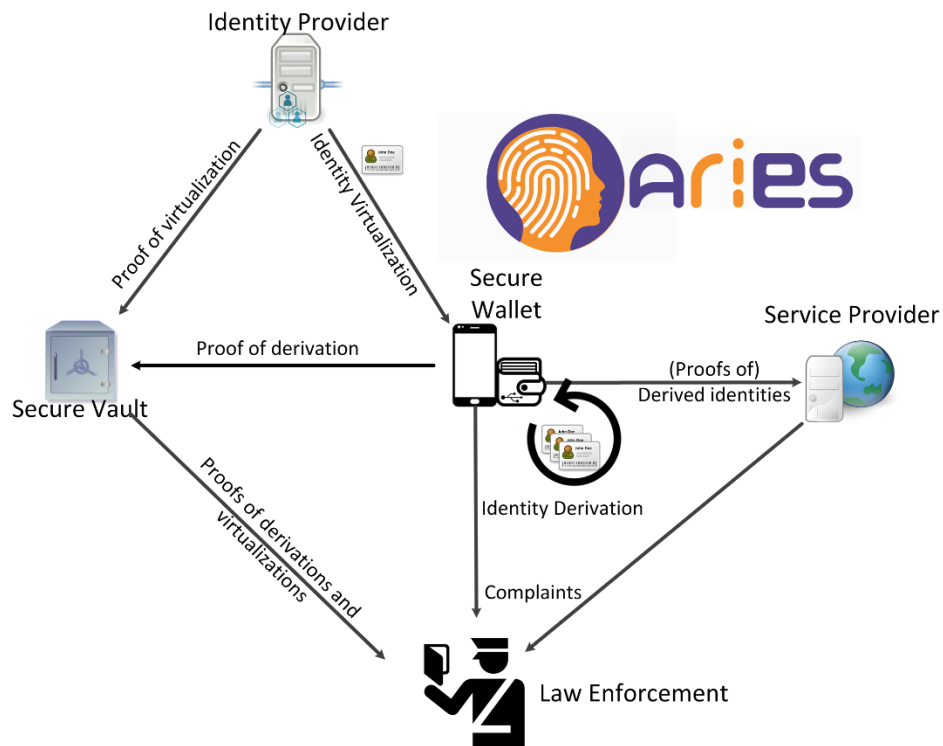
Figure 1: ARIES ecosystem.

The ecosystem will be demonstrated in two orthogonal real world use cases. In the first, ARIES will allow users to securely connect to an online commerce site, enabling a mutually trusted relationship without the need of disclosing non-essential personal data. The second use case will focus on the enrolment process and physical access control to a secure-sensitive environment such as an airport. The airport scenario will effectively show how different derived identities, with different levels of privacy, can be used in different situations (e.g., airport access control, boarding control and duty free shops) combining attributes with different levels of assurance coming from different identity and attribute providers (e.g., national eID or passport and electronic boarding passes).

In terms of social transformation factors, ARIES will contribute to lower several barriers, including end-user acceptance, by providing a secure and privacy by design enabled solution. ARIES will endow users with the ability to anchor trust on a secure and high level assurance infrastructure that will be used to derive additional virtual identities supporting different levels of privacy-preserving and anonymization capabilities but relying on a law enforcement mechanism to obtain effective support in the event of identity-related crimes. This will make users feel more secure in these eID ecosystems, which ultimately will encourage the use of electronic identities and increase the trust in, and adoption of, ICT and online services across the EU by both citizens and businesses.

ARIES is a project that specifically aims to prevent and reduce the risk of identity theft and fraud crimes. This is achieved by the means of cryptographic links between derived, virtual and

biometric identities and by the cryptographic proofs accessible at the secure wallet by law enforcement agencies that can leverage them when investigating identity crimes.

The ARIES project is a Research and Innovation Action funded by the European Commission's Horizon 2020 programme and the consortium carrying it out consists of a well-balanced mixture from six European countries consisting of industry partners, SMEs, public law enforcement bodies and also one retailer.

Links:

[L1] http://aries-project.eu/

[L2] https://twitter.com/AriesH2020

References:

[1] N. Robinson et al.: "Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime"

[2] European Commission: "The European Agenda on Security", COM (2015) 185 final.

[3] I. Naumann, G. Hogben: "Privacy features of European eID card specifications" Network Security, Vol. 2008.

Please contact:

Nicolás Notario
Atos Spain (Atos Research & Innovation)
E-mail: nicolas.notario@atos.net

Antonio Skarmeta
Universidad de Murcia
E-mail: skarmeta@um.es