Identity ecosystem

New technologies, processes and security features for physical and virtual identity management

Biometric identity

Strengthening the link between physical documents linked to the biometric and the digital (online and also mobile) identity

Impact

Address key legal, ethical, socio-economic, technological and organisational aspects of identity-related crimes

Atos

UNIVERSIDAD DE MURCIA

gemalto
security to be free

SAHER (UK) Ltd.

IDEMIA
augmented identity

ERTZAINTZA

Office of the Police & Crime Commissioner West Yorkshire

Politie Police

SONAE

@AriesH2020

www.aries-project.eu

aries

ReliAble euRopean Identity EcoSystem

Effectively reducing the risk of identity fraud and crime

www.aries-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700085

Objectives

Develop a trustable, reliable identity ecosystem for secure, ethical and privacy respecting physical and virtual identity management processes, with the aim of reducing identity fraud and associated crimes.

Strengthen the link between physical and digital identities by using high assurance elements, including biometric verification and tamper-proof certified checks with breeder documents.

Validate the ARIES approach in two realistic citizen-oriented scenarios: eCommerce and at the airport.

Address key legal, ethical and societal aspects of eID adoption and identity-related crimes to augment confidence in eID use.

Develop a secure infrastructure able to derive digital identities considering different levels of assurance

ARIES ecosystem will empower its users with a mechanism (identity virtualisation process) allowing them to generate virtual identities. These virtual identities will be simultaneously linked to the citizens' biometrics and to existing electronic and physical identities possessing a high level of 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, so avoiding usability issues and technological fragmentation (multiple standards) of physical identities and related technologies across Europe.

Validation scenarios:

The eCommerce scenario focuses on demonstrating how virtual identities with different levels of assurance can be used to access different online services and how the level of assurance may determine the operations that people are allowed to perform. This scenario will evaluate the effective control of citizens over their virtual identities, allowing them to enrol with the ARIES ecosystem and build separate identities, for different purposes, effectively minimizing the disclosure of data and maximizing their privacy.

The airport scenario includes use cases of online enrolment, online check-in and using the different partial identities for security control, police checks and airline checks at the boarding gate and the duty-free shop. It focuses on the process of issuing and linking virtual identities with their physical counterparts. Both, the virtual identity derivation process and its usage for physical and digital authentication purposes will be linked to citizens' biometrics, minimizing the risk of identity fraud.