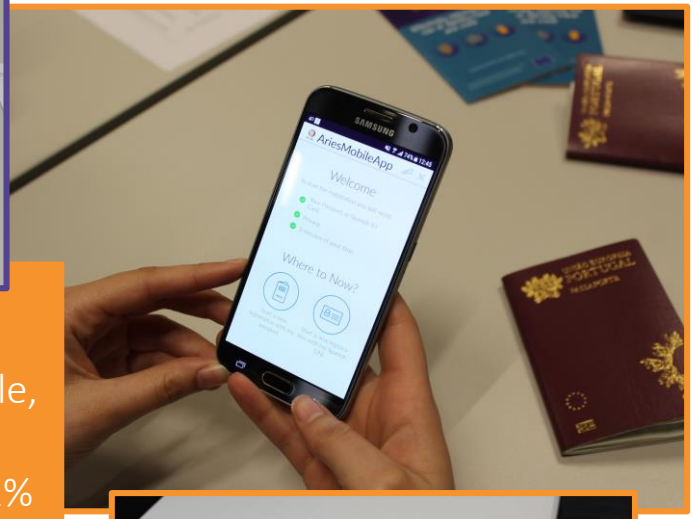
aries
Application of
Virtual Identities
in relevant societal and business context
aries
Effectively reducing the risk of identity fraud and crime

VID CONCEPT AND ECOSYSTEM

In general terms a digital identity is made up of a set of personal data such as an id number, name, address, biometric data etc. that can be used to represent a user to service providers both online and offline.



In 2017 the proportion of internet users, among EU people, ordering goods and services online reached the 68% and 52% of internet users provided personal data online.

Digital economy & society in the EU – 2018 edition (Eurostat 2017 surveys results.)

As physical ID documents, digital identities can be stolen, the personal information that made up one person's digital identity can be robbed and used for online banking or to purchase goods and services online.

Identity fraud rates have increased over the past years, in UK, in the first semester of 2017 it accounted for 56% of all fraud, and in particular 83% of identity frauds were committed online. The widespread use of online services is essential for building the digital single market but the access to online services must be aligned with European security and privacy requirements and regulations.

https://www.cifas.org.uk

aries project

reliable european identity ecosystem

"to develop and test secure technologies contributing to further establish a European electronic ID ecosystem trustworthy for the citizens. For that purpose, we will design easy to-use and privacy-preserving tools dedicated to identity management"

ARIES, "Reliable European Identity ecosystem", is a H2020 project that has received funds from the European Commission under grant agreement number 700085. ARIES addresses fight against crime and terrorisms in particular focuses on the research of new means and technologies for identity management with the specific aim of preventing identity theft and related crimes.

ARIES has a duration of 30 months. In the first phase of the project our efforts focused on the collection of the social, ethical, legal and technical requirements that leaded system design decisions and the definition of a security and privacy architecture. In the second phase of the project we have worked on the implementation of two system demonstrators on the eCommerce and travelers at the airport domains. All along the project lifetime the consortium has been engaged in continuous and cross cutting communication and dissemination activities aiming to raise awareness of the project among relevant stakeholders.

Achievements and distinctive features

ARIES promotes the use of national-wide identities, issued by trusted national authorities, as a baseline for citizen digital credentials that can offer high level of security against identity-related crimes. We have developed a secure infrastructure able to derive digital identities linked to eDocuments such as ePassports or electronic national identity cards, issued with the highest levels of assurance.

In addition, we provide tools and technologies to derive, for the same user, multiple digital identities with different levels of assurance to be used for different purposes but always supporting privacy-preserving and anonymization capabilities. ARIES incorporates biometrics for identity verification prior to the derivation of users' digital identities and for authentication when accessing a service. Biometric characteristics are unique and the best method to proof one person's identity. Live biometrics are almost impossible to forge so avoiding impersonation and identity theft. ARIES architecture supports the integration of different types of biometrics. In the project scope we have implemented demonstrators with two types of biometrics: live face and voice recognition.

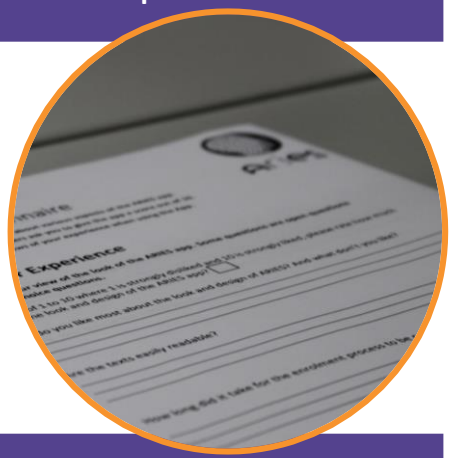
ARIES is compromised with the minimum disclosure principle with data protection and privacy requirements demanded by European institutions and citizens alike. GDPR establishes that natural persons should have control of their personal data and determine how that data can be used and by whom. ARIES enables users to reveal to service providers the information which is strictly necessary to provide their service without revealing any additional personal information. ARIES makes use of zero proof knowledge technologies, which ensure both privacy preserving authentication to citizens and compliance with access restrictions to service providers.

aries project
reliable european identity ecosystem

ARIES is an easy to use system which runs on mobile devices. It could be said that ARIES provides secure mobile eIDs and everything users need is a mobile phone. From their smart device they can create their digital IDs derived from physical official documents and authenticate themselves to service providers with the guarantee that the authentication process is run in a Trusted Execution Environment. All the identity management processes are performed from users' mobiles, even storage. Digital identities are stored in the user mobile phone in a secure wallet, cryptographically protected, for users' convenience preventing unauthorized disclosure or access to personal data by third parties.

IN ARIES WE ARE SERIOUS ABOUT OUR SOCIAL AND ETHICAL OBLIGATIONS

Efforts have been devoted to analyze social, legal and ethical requirements related to the use of digital IDs, basically, but not only, the analysis of eIDAS and GDPR regulations and the study of the overriding barriers to societal acceptance of eIDs



ARIES is neither the first nor the last attempt to build an ID ecosystem addressing citizens and administrations concerns raised about the management of digital identities and other cybersecurity dangers threatening the European Digital Single Market, but ARIES system possesses a set of distinctive characteristics and features enabling an efficient and convenient way to manage identities and providing tools to derive virtual identities supporting privacy preserving and security capabilities.

ARIES CONSORTIUM

The ARIES consortium consists of 8 partners from 5 countries combining a multi-disciplinary team and complementary competences inherent to large industry, research organizations, international service providers and law enforcement agencies.

INDUSTRY

Atos

gemalto
security to be free

IDEMIA
augmented identity

SERVICE PROVIDER

SONAE

SME

SAHER (UK) Ltd.

RESEARCH

UNIVERSIDAD DE MURCIA

LAW ENFORCEMENT

Office of the Police & Crime Commissioner West Yorkshire

ERTZAINTZA

Politie Police

Challenges and Opportunities of the Market

Cybercrime, **identity theft** and the **fraudulent use of identities** are growing threats stemming from today's increased use of new technologies for financial transactions and the greater movement of people across borders. In both regards, the traditional printed passport or identity card are increasingly inadequate documents in a world in which technological solutions are clearly the way forward. Criminals are growing more sophisticated in the means of attack and the rewards are growing. In addition resource and skills issues place increasing demands on law enforcement agencies and these types of crime are difficult / expensive to investigate and detect. It is much better for all concerned to work collaboratively to increase resilience to attack and prove the adage "prevention is better than the cure".

Challenges

The big challenge for the providers of any e-service is reconciling business opportunities opened by interoperability and infinite information linkage with the need for privacy and security. Balancing privacy and security alone is an business opportunity for providers as this is the external face of their work commonly seen by citizens - we are all familiar with claims to protect our privacy through secure technologies. But that is not even only half the story.

Security and privacy cannot simply be seen through the prism of data protection legislation and robust algorithm and data handling. Rather, the actual purpose and use of the data acquired as part of service provision poses ethical challenges that are commonly overlooked. This is a major and common business model risk because ultimately failure to address ethical matters risks undermining the business opportunities and models by inadvertently allowing public confidence and trust in the application and provider to drip away. Citizen disenchantment with data breaches or unconsented information linkage encourages citizens to drift away from a service.

↳ aries therefore seeks to provide a route to boosting citizen and confidence in using online services from private, public or private public partnerships achieving that is a goal of the EU's digital single market

For service providers in the policing and security sector, the priorities will differ from those providing commercial online retail services. For the former, optimizing the chances of having certainty in the claim to an asserted identity is critical to combating and prosecuting crime of any sort. For the latter, certainty in the capacity to pay of someone seeking to acquire a service is crucial. Accordingly, challenges and priorities in eiDs differ.

In both industry and law enforcement sectors interest has grown exponentially in using biometrics to increase certainty that a claimed identity corresponds to a genuine person entitled to claim that identity. However, the ethical questions of disproportionate use of biometrics for trivial purposes threatens to undermine public trust and confidence in the service and the provider using them.

A major challenge for a society facing such a complex scenario is to put a complementary biometric identity verification system (fingerprint, facial, voice & iris recognition etc.) in place. Whether shopping online, dealing with the administration or travelling internationally, for all those involved (individuals, retailers, public sector institutions and security forces etc.) the importance of a reliable and tamperproof identity verification system cannot be overstressed.

The challenge for biometric system developers is to develop a solution which meets a wide variety of needs. First and foremost, the system should be citizen friendly and is both easy yet secure to use, while proving sufficiently robust for service providers and security forces.
Secondly, speed of verification and ease of use are essential elements, e.g. the system should allow for seamless cross border travel, speeding up the process for both travelers and security staff.

↳ Under pinning the ultimate global success of any system such as aries is the authenticity of the breeder/source document from which a claimed identity is derived.. (birth certificates, national identity cards, passports and/or visas etc.)

regarding technical compatibility, any system should work with all common platforms and devices and be easily updatable.

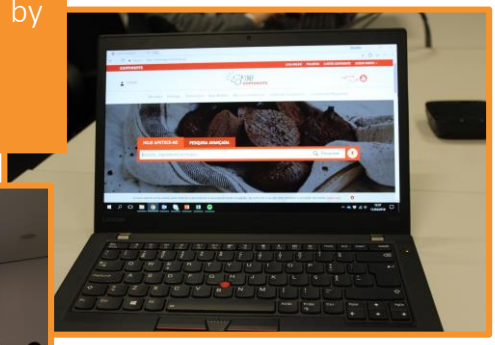
opportunities

In addition to help combat ID theft by making citizen for resilient to attack, the implementation of such an identity verification system would have a significant impact on the way we go about our everyday lives. For example, journeys to sign documents such as mortgage papers could become unnecessary, thereby freeing up people's time and putting less burden on transport systems. A further example is that citizens in some countries currently need to visit a police station to ratify complaints filed online, a step which again could be avoided with a biometric ID check.

↳ Given the great potential of biometric id systems, and if the challenges are addressed, then the opportunities for business are clear.

real life applications
e commerce

The secure eCommerce scenario focuses on demonstrating how virtual identities with different levels of assurance can be used to access different online services. It shows how this level of assurance may determine the operations that people can perform. It demonstrates the control citizens have in practice over their virtual identities, allowing them to enroll with the ARIES ecosystem and build separate identities, for different purposes, effectively minimizing the disclosure of data and maximizing their privacy. This is informed by and designed to ensure implementation of ethical principles to help build trust.



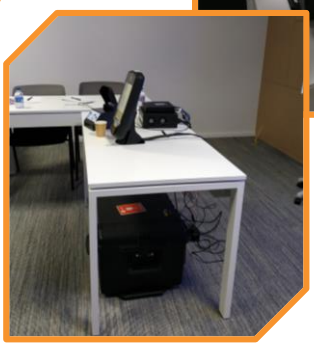
In the registration process the user can link real physical identity with the Aries vID through the breeder document this means increased level of assurance of the identity. User proofs his real Identity through biometrics, matching the fresh live capture of his biometrics with the ones stored in the breeder document. This may be used in case of some limitations (some goods have age limitation) and lowers risk on eCommerce organization side. This registration process provides additional security enforced by cryptographic means of the ARIES vID token. In addition, it enhances privacy, as user has full control over his data and threats of data stolen from IdP or eCommerce website is lowered.

During authentication, users are empowered with stronger mechanisms as additional authentication factor (biometry) is accomplished, and user has full control over his information.

real life applications
airport

This scenario shows, under realistic near-operational conditions, how ARIES technologies can be used to prevent and reduce the risk of identity fraudsters to physically impersonate victims and to take advantage of identity issuance procedures provided to legitimate citizens, to commit identity crime and fraud bypassing physical access control measures.

This scenario will allow users to build sets of virtual mobile identities, cryptographically protected and securely derived by means of a highly secure process from physical official identity/travel documents, which have been issued under strict assurance conditions by authorized entities. This process will be strongly linked to the derived mobile virtual identities, to the physical breeder document and the unique biometric characteristics of the citizen or involve LEA officers at the airport in case the breeder document has been lost or stolen.



Work ahead

The project provided an architecture, example implementation of the solution and collected feedback from test users. Moreover it collected and summarized all requirements that may arise during production of the project which would provide a good guidelines for any organization that would like to deploy and operate an Aries solution. The architecture and the implementation provides basic building blocks, but there are still points that must be addressed by application deployment and organization of operations to provide level of security and privacy the project means to address and that is enforced by GDPR.

According to user feedback from pilots the solution would be accepted by young technically skilled generation without any issues, but there were improvements identified to allow wider acceptance. The user experience should be fine-tuned for several steps of the registration flows, where especially the ID Proofing step and biometric enrolment were not intuitive, because they were the main advancement of the project with no example of widely used application on the market.

The project pilots were run on selected set of handsets in a more or less controlled environment, so it is also expected that anyone opening Aries solution would also need to work on handset support. The handsets on market have very various technical parameters which would require a lot of development work especially for the biometric authentication where the reliability is affected by quality of handset.

Even though there is a lot of work up to any future Aries operator, the solution seems promising and may be a good addition to existing authentication solutions, where it can easily position itself above existing social network logins, where it can provide much more reliable identity, and below eID or eIDAS based authentication solutions, where it provides less official but more user friendly authentication with additional security of biometric authentication.

There are two directions future evolution of Aries may continue.

Another evolution path is the boarding use case. The project explored possibilities of the case, but there are still questions to be answered. The pilot did not provide a clear path how to start cooperation with airlines. In the user tests we used simplified flow with a scaffolding between the airline App and the Aries App. Discussion with airlines with a bigger focus on integration may be done and a sample pilot with their direct participation may prove Aries defines a simple and clear integration path.

The architecture provides a framework that may be used to combine new authentication methods and flows, it provides a guideline how to bind biometric authentication and cryptographic scheme, so it may be used as a playground to explore and introduce new approaches with a guarantee of certain level of security and privacy. It may be expected that soon new biometric features will be invented, each of them with a specific advantage over the others: usability, intuitiveness or security, and Aries provides a way how to quickly introduce them without the need to invent the overall deployment model.

The boarding use case itself as implemented in Leeds-Bradford airport showed several usability limitations such as QR code reading issues addressing which may lead to many improvements of currently used systems and new design approaches to use cases when user is offline and needs to share information with online terminal.

In overall, the project provided many outputs that may be used in many ways either as a proof of concept, example of implementation or important requirements every authentication solution may face. Even if the project would not be exploited in future as it is, it provides a value to those interested in user authentication.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 700085