11

An Overview on ARIES: Reliable European Identity Ecosystem

Jorge Bernal Bernabe[1], Rafael Torres[1], David Martin[2], Alberto Crespo[3], Antonio Skarmeta[1], Dave Fortune[4], Juliet Lodge[4], Tiago Oliveira[5], Marlos Silva[5], Stuart Martin[6], Julian Valero[1] and Ignacio Alamillo[1]

[1]University of Murcia, Murcia, Spain
[2]GEMALTO, Czech Republic
[3]Atos Research and Innovation, Atos, Calle Albarracin 25, Madrid, Spain
[4]Saher Ltd., United Kingdom
[5]SONAE, Portugal
[6]Office of the Police and Crime Commissioner for West Yorkshire, (POOC), West Yorkshire, United Kingdom
E-mail: jorgebernal@um.es; rtorres@um.es; martin.david@gemalkto.com; alberto.crespo@atos.net; skarmeta@um.es; dave@saher-uk.com; juliet@saher-uk.com; tioliveira@sonae.pt; mhsilva@sonae.pt; stuart.martin@westyorkshire.pnn.police.uk; julivale@um.es; ignacio.alamillod@um.es

Identity-theft, fraud and other related cyber-crimes are continually evolving, causing important damages and problems for European citizens in both virtual and physical places. To meet this challenge, ARIES has devised and implemented a reliable identity management framework endowed with new processes, biometric features, services and security modules that strengthen the usage of secure identity credentials, thereby ensuring a privacy-respecting identity management solution for both physical and online processes. The framework is intended to reduce levels of identity-related crimes by tackling emerging patterns in identity-fraud, from a legal, ethical, socio-economic,

technological and organization perspective. This chapter summarizes the main goals, approach taken, achievements and main research challenges in H2020 ARIES project.

11.1 Introduction

In a world getting every time more and more digital, the protection of the personal data is a crucial point, in particular, individual identities are vulnerable in this scenario, where European stakeholders are interacting in a global way. The lack of trust is increasing derived from the current absence and deficiency of solutions, including consistently applied identification and authentication processes for trusted enrolments, particularly the use of online credentials with low levels of authentication assurance. Moreover, there is not a common approach in Europe (from the point of view of the legislation, cross-border cooperation and policies) to address identity-related crimes. This situation costs billions of Euros to countries and citizens in fraud and theft.

In this scenario, ReliAbleeuRopean Identity EcoSystem (ARIES) H2020 research project aims to provide a stronger, more trusted, user-friendly and efficient authentication process while maintaining a full respect to subject's and personal data protection and privacy.

Thanks to this ecosystem, citizens will be able to generate a digital identity linked to the physical one (eID/ePassport) using biometrics while, at the same time, store enrolment information in a secure vault only accessible by law enforcement authorities in case of cybersecurity incidents. Because of this process, linking proofs of identity based on the combination of biometric traits and citizen digital identity with the administrative processes involved in the issuance of documents like, for example, birth or civil certificates will be possible.

Users will also be able to derive additional digital identities from the ones linked with their eID or ePassports with different levels of assurance and degrees of privacy about their attributes. The new derived digital identities may be used in administrative exchanges where it is required by the governments according to eIDAS regulation [1] and be store in software or hardware secure environments in their mobiles or smart devices.

The rest of this chapter is structured as follows. Section 2, depicts the ARIES Ecosystems, Section 3 is devoted to the main innovative process in ARIES. Section 4 describes the legal and ethical approach considered. Section 5 recaps the main cyber-security and privacy Research challenges. Finally, Section 6 concludes this chapter.

11.2 The Aries Ecosystem

The project goal is to provide new technologies, processes and security features that ensure a higher level of quality in security aspects like credential management for privacy-respecting solutions and the reduction of identity fraud, theft or wrong identity problems which can be associated with crimes. The general Aries ecosystem is depicted in Figure 11.1.

Authentication processes will be ensured with the use of smart devices allowing to use all required biometric (especially face) and electronic (using NFC) data. This process should ensure a high level of quality for biometrics acquisition, while assuring data integrity and delivering the derived identities required attributes to the adequate relying party (service provider). Such features will be achieved by functionality locally (on the smart device) or centrally (back-end). Moreover, digital identities will be generated with privacy preserving technologies and allowing citizens to just prove to be in possession of some attributes without exposing the rest of their data, i.e. being over 18 years old. Given that different levels of assurance are possible a biometric mechanism could also be used as a proof of digital identity possession where appropriate.

A user manages multiple identities and credentials which are issued by Identity Providers (IdP) and presented to the Service Providers (SP) to access the offered services by them. The ARIES approach considers a multi-domain interaction for eID management in order to achieve a distributed but unified eID ecosystem. Each domain usually contains one or more IdPs and one or

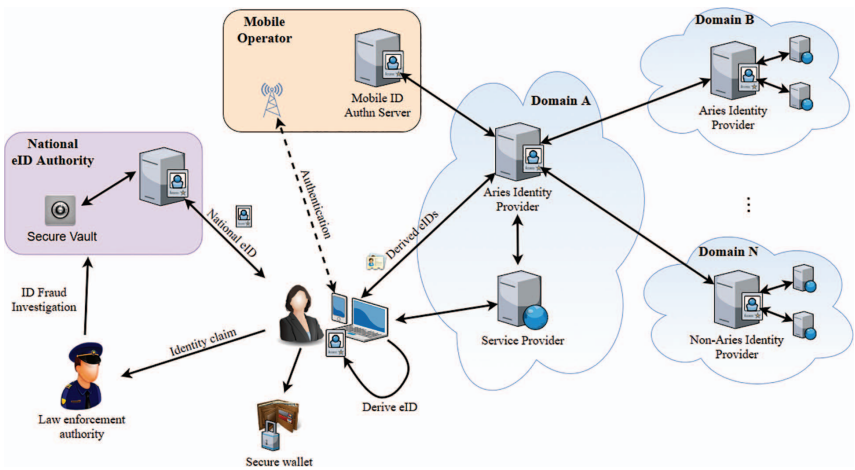

Figure 11.1 ARIES ecosystem overview.

more SPs. Usually, a SP redirects the user requests to the IdP within its own domain but there are some exceptions to be considered: An SP can directly authenticate the identity of the user (e.g. validating a certificate) and could, also, redirect to an IdP of another domain in which it trusts, including a mobile operator, a bank or a Government for Mobile eID authentication. In addition, IdPs can be interconnected relying on federated interoperability, thereby allowing delegation of authentication (e.g. using STORK) and also attribute aggregation (e.g. to create a derived credential which includes both governmental and academic information). User consent will be obtained prior to transferring any personal information. Interaction with legacy non-ARIES IdPs can be also achieved by contacting those IdPs via standard protocols such as SAML [2], OAuth2 [3], etc.

The users interact with the system through several devices such as mobile phones or smart wearables. These devices will require a secure element in order to securely protect digital identities with biometric features. Alternative, although less secure, storage and execution environments might be foreseen for larger adoption of the ecosystem, but with limited capabilities to manage the resulting risk. A secure electronic wallet will be provided to users for them to securely handle and manage their digital identities and their related data.

New derived credentials can be requested by users to an ARIES IdP after an authentication process using its eID. These credentials may contain different identity attributes and/or pseudonyms, according to the user needs and required level of privacy and security. The issuance process implies that the new credential must be issued by a trusted IdP and logged to assure the traceability in law enforcement purposes such as real identity identification. This could be achieved by an encrypted and signed logging mechanism. The logged information should also be kept secured and only accessed due to law regulated cases.

The derived credentials will be originated from previous strong ones such as biometric data and eID documents. The process is based on mobile token enrolment server with a derivation module. Optionally, users could also derive their own identity and present cryptographic proofs to an SP. In this case, identity approaches based on Zero Proof Knowledge Proofs like IBM Idemix [4] or ABC4Trust [5] solutions can be used. For this, the obtained credentials should be prepared with the needed cryptographic information to derive new identities and provide proofs when requested by an SP.

Those identities can be derived and issued by different entities having, each credential, an associated Level of Assurance (LoA). This serves as a measure of the security mechanism used by the credential issuer to validate

the user identity. ARIES aims to keep the LoA or to avoid significant differences when using derived credentials and similarly, will try to ensure that Level of Trust (LoT) among different entities is also a maintained after adopting derived credentials in the ecosystem.

Accessing a service provided by an SP will impose some requirements for the credential to be presented, like including some attributes about user identity and other trust requirements. The user can choose the mechanism and the credential which he wants to present according to his preferences and the required information by the SP. This includes the usage of derived credentials or pseudonyms with less exposed information; a proof of identity in which no credential is actually sent to the SP, but a proof that the user owns some identity or attribute; or a Mobile ID credential stored in a secure element, which makes use of the Trusted Execution Environment for authentication and can optionally involve mobile operator as party involved in circle of trust [6].

Privacy by design principles is essential from the data protection perspective especially when identifying which and how biometric data are going to be used. Indeed, the requirements of proportionality have to be analysed, bearing in mind the demands of technical security measures, determining what is certainly essential to avoid identity thefts based on the access to biometric information (e.g. a photo in the case of face or a latent in the case of fingerprints).

Likewise, the possibility of using several derived identity credentials demands a concrete assessment from the perspective of data protection. Therefore, it will be necessary to build up identification services prioritizing those technical and organizational solutions that minimize access to personal data to the absolute essential. To accomplish these objectives, ARIES devises means to comply with the minimal disclosure of information principle. In this sense, the principle of proportionality will play a key role in order to face this challenge, since it will be necessary to justify in each case by the service providers the personal data really required for authentication or authorization.

Furthermore, the identity ecosystem will provide unlinkability at the relying party level through polymorphic user identifiers (when compatible with relying parties' authentication policies). For each authentication or for specified periods of time will be different and random identifiers, so it will disclose no information. The unlinkability at the ARIES IdP will be also ensured. The ecosystem will indeed hide the accessed service from the enrolment and authentication services. Unobservability will be ensured by the system architecture as well. The Identity Providers will have no information about which SP the user wants to log into.

11.3 Main Innovative Processes in Aries

11.3.1 Fraud Prevention and Cyber-crime Investigation

The topics of fraud and crime prevention and investigation were one of the main project goals and were addressed from the very beginning of the project by involving law enforcement personnel in the process of requirement definition. Their inputs were based on currently most frequently occurring threats and their experience from crime investigation, and based on them an assessment of state of the art authentication architectures was done at the beginning of the design phase.

Main results of the assessment resulted in three main improvements in the field of crime prevention and investigation the project may provide:

- Strong authentication accessible to large part of the population to replace legacy authentication types (such as password or SMS one-time code).
- Biometric authentication as additional obstacle for the criminals.
- ID Proofing with document reading and biometric verification as a strong identity verification means to ensure the newly issued privacy preserving partial identities are based on reliable information.

It is obvious the strength of the whole solution depends on algorithms used for biometric verifications (both live capture vs. image data from electronic document and live capture vs. previously enrolled baseline template). This was in line with the project plan as improvement of both enrolment and verification of face biometrics was planned as a separate task.

If the authentication is broken by some means and the investigation takes place it usually requires as much information as can be obtained (IP address, device fingerprints, all transaction data) which is in contradiction with project goal to provide privacy friendly solution. It was decided the privacy and a control over user's own data is more important than inputs for investigation and a limitation was introduced. User data stored inside of the system are encrypted and stored in an appliance called Secure Vault. The appliance enforces strong authentication and authorization based on ARIES authentication, so it is only the user himself who can approve access to his data. This limits the investigation to cases when user's identity was stolen by forgery, but he still has access to his mobile phone to be able to provide access to law enforcement authorities.

The data collected and stored by all server-side components of ARIES solution consist of transaction information and anonymized identity information such as links between the cryptographic and biometric identity parts.

It was decided to introduce a rule that biometric information may be persisted only in user's handset in order to give him control over this most important information.

11.3.2 Biometric Enrolment and Authentication

The architecture considered that the biometric authentication is evolving and new methods and implementation are introduced as fast as the old ones are broken by new approaches such as deep learning. The solution is a set of loosely coupled server components that allows simple replacement of each component without much impact on the existing ones. To integrate with ARIES each vendor must provide server side API and App SDK, the project provides enveloping App with UI flow control and a server application that controls the issuance and authentication flows and ensures all steps happen in a single session. The choice of which biometric feature should be enrolled is based on user's choice and his handset capabilities.

The implemented OpenID Connect authentication flow allows selection of any available biometric authentication type, so the requesting Service provider may choose the optimal balance between level of assurance and user experience that may be worse for some biometric features.

The project considered two options of biometric authentication: usage of the feature obtained during ID Proofing process (at the moment only face image is accessible for commercial applications) and usage of another feature as an additional authentication factor without link to the original electronic document information.

The face recognition done during ID Proofing strongly relies on quality of the image from electronic document. During project pilot phase issues with several passports with poor quality image data were encountered that prevented enrolment of the users. The liveness detection is in ID Proofing mandatory, because if the attacker has stolen document then he gets hold of the image data himself, so the liveness detection is the only protection.

Pilot implementation used face recognition combined with ID Proofing and the results were satisfactory:

- Enrolment was successful for majority of the users and was done without issues on the first try.
- Authentication with liveness detection based on head movements (vertical and horizontal) using overlay image to tell the user what to do was smooth and well accepted by the pilot users. Average face verification time was below 3 seconds.

Voice authentication was implemented to prove the solution is able to quickly integrate an existing biometric authentication service. Existing server-side service proposed by one of the partners was selected and integrated in two steps: scaffolding REST service was created to align the API style and session management and very simple App SDK was implemented and added into existing ARIES App.

11.3.3 Privacy-by-Design Features (Anonymous Credential Systems)

ARIES follows a privacy-by-design approach to protect user's privacy in their digital transactions, either online or offline (on-situ, face-to-face interactions). The architecture has been designed to incorporate and interface with Anonymous Credential Systems (ACS), namely Idemix [4]. ACS allows users to set-up and demonstrate Zero Knowledge crypto Proofs, thereby proving certain predicates about personal attributes in a privacy-preserving way, following a selective disclosure approach.

The ARIES Mobile App allows obtaining ACS credentials, once the user has been identified and enrolled in the ARIES IdP. Those credentials are generated based on the attributes demonstrated by the user against the IdP during the ID-proofing, i.e., it contains at least the attributes included in the breeder document (ePassport) used for authentication and enrolment. The credentials are maintained securely protected inside the mobile (mobile wallet).

Once the user has performed the issuance protocol, it can create different proofs of possessions to comply with attributes required by the Service Provider to access a service. This presentation protocol is based on ZKP by relying on the CL signature scheme [7]. It ensures minimal disclosure principle, allows demonstrating having an attribute without disclosing the value itself, and permits proving complex predicates about attributes, e.g. the date of birth is greater than certain year (to check age). Anonymous credentials systems have been also integrated, and successfully evaluated, for IoT scenarios [8] in even constrained IoT scenarios [9] in the scope of Aries project.

In ARIES these privacy-preserving capabilities have been showcased in the Airport scenario, in which the user wants to demonstrate he is over 18 to buy certain products (e.g. alcohol) in a duty-free shop inside the airport, and prove that he has a valid boarding pass (required to buy goods) without revealing any personal data, proving only he is traveling to a valid destination in a valid time-frame.

11.4 The ARIES Ethical and Legal Approach

11.4.1 Ethical Impact Assessment

ARIES focussed on how to optimise the potential for minimising and averting unintended misappropriation and disproportionate use of information for unknown and diverse purposes to which citizens have not explicitly consented. It did so in ways that bring privacy and security in balance while addressing the socio-ethical consequences of deploying the ARIES solution to creating a reliable, trustworthy eID ecosystem.

ARIES also has as its foundations the EU's ambitious commitment to realising a Single Digital Market relies on creating trustworthy eIDs to augment efficiency, convenience and trustworthiness of e-life for citizens. Digital by default is enabled by the once-only principle (to cut multiple entry of same data several times), interoperability by default, inclusive and accessible practices.

11.4.2 Technological Innovation Informed by Ethical Awareness

Technological innovation is not neutral in conception, in development or in its application to society. Algorithms are not neutral. This is the starting point for reflecting on the ethical tests that might be applied as a new application is developed or an existing one extended and used for a different, but possibly complementary purpose, to the one for which it was first developed. Just because a development or application meets current legal privacy requirements, it cannot be assumed that it automatically complies with ethical standards that society values. This means that there must be clarity over the purpose of a new development and its intended used in real-time and in the real-world. The legal tests of ensuring compliance with the law provided by privacy impact assessments themselves are useful check points. By themselves, they are inadequate. Legal compliance is necessary but not sufficient to ensure ethical standards are met.

11.4.3 The Socio-ethical Challenge

The key challenge for ARIES was to develop something that was universally acceptable, complied with legal and ethical requirements, while protecting security and privacy and would help form the basis of a reliable and trustable eco-system. Accordingly, ARIES set about developing a neutral application that sought to facilitate convenient, privacy respecting, secure, and speedy transactions whilst minimising the amount of personal data that an individual

citizen might be required to disclose (by choice or design) in order to access a service.

11.4.4 ARIES Starting Point: What is Meant by Ethics?

The ARIES ecosystem is designed with both privacy and ethics in mind. ARIES extracted core principles of ethical practice from philosophy and medicine which have addressed the impact of technical and scientific advance on what it is to exist as a human being. There is no universal acceptance of what is ethically appropriate or acceptable. Consequently, designing something that is 'ethical by design' implies designing something that minimizes objections to it from different societies and is an essential building-block of an ethical e-ID eco-system.

The do no harm principle provides the best initial ethical test to be applied to the design of a new algorithm or app. It is useful for a digital society accustomed to automated decisions being driven by bots rather than immediate live human decision making on a human2human basis. However, this immediately raises additional ethical issues summarized by the principles of proportionality, purpose specification and data and purpose minimization. Dignity and autonomy are core elements of the concept of bodily integrity. To those are added notions of privacy (in private and public transactions).

In short, the use made of something, like an eID, occasions many ancillary questions about the person associated with it. This is problematic and has preoccupied legislators and citizens anxious to ensure that they do not inadvertently reveal and allow to be sold for commercial gain, aspects of themselves (i.e. data and associated information that they generate). Further ethical issues arise. Therefore, ARIES seeks to develop a solution which bakes in ethics and is as neutral as possible in its impact on societal values.

11.4.5 Embedding the Dominant Ethical Principle: Do No Harm

The key ethical principle to which all other ethical principles are linked and subordinate is the pre-cautionary principle. It highlights the obligation to 'do no harm'. Closely associated and derived from it are principles impelling proportionality, self-determination and consent, autonomy, dignity, and necessity (data minimisation). Refining accepted medical ethics for informational technology practices suggests that ethical practice and ethical technological applications need to be aware of, and in the case of eIDs, sensitive to how they will mitigate, avert or accommodate risks (or potential harms).

The precautionary principle of do no harm is about more than determining legal liability and redress for harm. In ARIES, it informed design and practice from the start. This differs from the traditional practice of using legal remedies for harms, and the focus in the USA, for example, of litigation to provide financial recompense for harm. In ARIES, attempts were made to widen the understanding of what 'harms' might be induced by ICT innovations in line with the EU approach to baking in the precautionary principle of 'do no harm'. In the EU, this is expressed in guidelines and in legislation which translates this principle into duty-of-care provisions, as in the case of the GDPR and the complementary ePrivacy Directive (soon to be Regulation). This duty-of-care has been marked in respect of privacy protection in both the GDPR and ePrivacy deliberations: both require importers and retailers of IT to distribute only privacy-by-design compliant technology. The temptation to assume that PbD compliance automatically implies respect for ethical principles must be avoided.

For ARIES ecosystem, ethics is seen in relation to when, how and by whom (or what algorithm) decisions are made, and for what purpose. This means that there are several points at which ethical reflection must occur in order to guard against baked in bias and ensure ethical principles are respected in terms of all elements of the design, from inception to roll-out, to scalable use. Such ethical checks occur at the following points: design of the medium in which personal information is to be held; technical rules governing handling or and access to that information, including via a human or bot; technical vulnerability to the integrity of the medium and its message; commercial opportunities; and impact on the individual providing information (knowingly or not) to access a service. ARIES reflected on how ethical principles may be used to inform data handling practices that rely, at some point, on eID authentication on the part of the individual or the service provider.

Core ethical principles to be observed are: precaution; proportionality; purpose specification; purpose limitation; privacy; security; autonomy; dignity; informed consent; justifiability; fairness; transparency and equality.

11.4.6 Baked in Ethics for the ARIES Use Cases

The ARIES Use Cases on eCommerce and e-Airport reveal that different rules apply to eID based transactions in a common physical setting owing to pragmatic and political constraints imposed by real-world contexts, real-time eID development and use. These values, so far, are shaped by human beings.

For the ARIES, the baseline was the ethical principles common to our societies in the EU28, awareness of what the public interest is; how it can be explained and protected. This entailed learning from on privacy assessment initiatives, regulations, oversight mechanisms, audit, inspection and compliance arrangements and independent scrutiny to ensure accountability and redress. Implicit are ethical principles of good governance, transparency of intent and effect. This places a premium on minimum disclosure requirements in terms of how algorithms are designed and used, phased and shaped (often by other automated processes) and deployment that is proportionate to the goal they are designed to attain. Ethical compliance is not met, therefore, simply by assuming, especially in the case of eCommerce, that competition and anti-trust legislation, standards and regulations are sufficient to guarantee ethical use. Nor is accountability just about liability for malfunction or misuse. This is why the baking in of ethics, an ethic audit trail even, mean that accountability has to be citizen focused and relate also to the intended use and effect of using an eID on society.

Ethical eID design therefore must reflect principles of accessibility, dignity, equality and transparency. Ethical design suggests that in practice where eID use fails to be used, for whatever reason, there should be clarity over why this happens and, in order to preserve dignity and accessibility, alternative means of completing an intended benign transaction. The GDPR Art 22 states that people have a right NOT to be subject to a decision 'based solely on automated processing'.

11.4.7 Ethics in the ARIES Use Cases

ARIES Use Cases rested on the same set of questions and methodological approach to ensure consistent application across all of the ARIES activities. All checked fitness-for-purpose. How is ethical use designed into the system? What bias is there? How can risks and benefits be reconciled? How have ethics been designed into the technical solution envisaged? Is this sufficient from the point of view of user trust building? ARIES was especially mindful of the inherent risk of doing inadvertent harm. Its Ethical Impact Assessment tool therefore reflects this by highlighting that any data enrolment, collection or (manual or automated) processing must not harm the data subject directly or indirectly. It must be proportional to the purpose for which processing occurs, must minimise data used and ensure that it is used for that one, specific and limited purpose only. No more data should be enrolled or collected and associated than is expressly necessary for the transaction envisaged.

Breaching the spirit of privacy preservation under the GDPR is a breach of ethical practice.

ARIES concludes that an EIA is a commercial opportunity in its own right and key to building sustainable trust and reliability while maximising privacy and security. An EIA should be conducted in parallel with PIAs. An Ethics audit via an independent and expert body should complement a PIA. These should be done before the decision to proceed with further development of the technical solution is taken. It must be done at the outset (possibly after taking external, independent advice) and authorised and signed off at the highest level. This helps create a trusted privacy and ethics respecting environment for developing innovative technical solutions. Ethically informed good practice becomes second nature. This is communicated to the public and stakeholders. Public trust is key to sustaining trust in the reliability, security and dependability of the solution.

11.4.8 Legal Challenges and Lessons Learned in ARIES

As explained in precedent sections, ARIES proposed the use of new identification techniques, fully user centric, that required a complete review of the different legal framework that may be considered applicable to the service, in case of real exploitation.

First of all, an analysis of the eID European Union legislation, and its application to the ARIES ecosystem was conducted, mainly focused in the Regulation (EU) N° 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (commonly known as "eIDAS Regulation") and its implementing acts.

Our findings include that an ARIES provider may play two different roles in the eID EU regulated ecosystem:

- First of all, an ARIES provider may be an electronic identification means consumer. This happens when the ARIES provider uses the electronic identification means issued to the citizen i.e. by the Member State, such when the citizen authenticates using a national citizen ID card (i.e. the Spanish National ID card, or the German nPA). This is an interesting way to reuse strong authentication-based identification mechanisms as an authentic source for the self-issuance of user-controlled identities.
- Secondly, an ARIES provider may be an electronic identification means issuer, in the sense of the eIDAS Regulation. For this to happen, the system must comply with the legal requirements set forth by the eIDAS

> Regulation, and the corresponding implementing acts, and be recognized by a Member State. The ARIES derived identities aim to be recognized according to the substantial security level defined in Article 8 of the eIDAS Regulation and, thus, the system shall comply with the corresponding requirements set forth in the eIDAS Security Regulation. This possibility would allow the usage of the ARIES derived identities for the electronic access to public services in the EU.

Due to their nature as a private, pseudonymous, identification means with legal value under eIDAS Regulation, an analysis of the use of advanced electronic signatures based in qualified certificates issued by ARIES providers was also considered relevant, for the endorsement of derived identities. Research concluded that an ARIES provider may issue qualified certificates assuring the identity of the person, using pseudonym certificates and other attributes, as a means to represent derived identities. This possibility is directly implementable in the current EU framework, but its recognition is subject to the authorisation of the usage of pseudonym certificates in each Member State.

More interestingly, our research showed that an ARIES provider could offer a new trust service, consisting on the accreditation of possession of personal attributes (a wide conceptualization of identity) with privacy protection.

This may be considered as the main legal innovation of the project: an ARIES provider, once a person identity has been provisioned, provides a service that allow that person to self-create partial, derived, identities asserting in a trustworthy manner a particular personal attribute (i.e. the possession of a personal, valid, boarding pass to shop in the airport, or being older that certain age…). These derived identities constitute assertions that may legally substitute the corresponding documents that evidence the personal attributes (i.e. instead of showing the boarding pass, with all personal data, one shows a partial, derived identity that proves the fact that the person has a personal and valid boarding pass), thus increasing privacy effectively, while reducing compliance costs to data controllers.

To be able to substitute these documents per partial derived ARIES identities, maintaining legal certainty, a definition of this services a new trust service should be proposed, including the institutionalization of the service and a legal effect attained to the service (i.e. establishing some sort of equivalence principle such as "where the law requires the documental accreditation of a personal attribute, it will be possible to use a [service name] evidence".

11.5 ARIES Ecosystem Validation

11.5.1 E-Commerce

The secure eCommerce scenario focused on demonstrating how virtual identities with different levels of assurance can be used to access different online services. It showed how this level of assurance may determine the operations that people can perform. It demonstrated the control citizens have in practice 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. This was informed by and designed to ensure implementation of ethical principles to help build trust.

The e-Commerce demonstrator scenario overview and main processes identified are shown in Figure 11.2. The demonstrator allowed users to use their own eID's present in the ARIES vault to register and to login using their biometrics (face authentication) on the Chef Continente website. This new authentication method was done in the mentioned website using the ARIES system and app to read real documents (e.g. passport) and biometrics (user's face) to validate identities and connect to the third-party e-Commerce service from Continente, the Portuguese leading retailer.

The demonstration stage aimed to validate ARIES' results in terms of applicability of the resulting ecosystem and enabling tools and technologies and effectively demonstrate the progress beyond the state of the art of ARIES achievements in a realistic scenario having potentially high impact on society

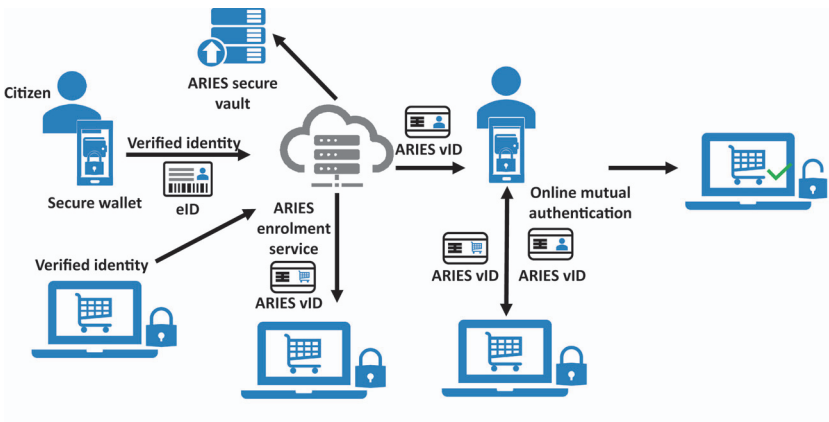

Figure 11.2 e-Commerce demonstrator scenario overview.

and the economy (this stage was done under strict ethical and legal requirements to protect participants). Several tools were used and are presented next in chronological order:

1. The ARIES Online Survey was designed to ascertain citizens' expectations of the ARIES eID and inform the project about which issues needed to be addressed (222 respondents);
2. Proof-of-Concept Design Thinking Workshop had the objective of to engage potential users with the ARIES system and get their feedback about relevancy, usability and functionalities (16 participants);
3. The Demonstrator Focus Groups stage had the main goal of testing the ARIES app in the real context with a group of users that had different backgrounds, ages and experiences (29 users).

The demonstrations were done amidst a time were the concern about privacy and security was at its highest, as this testing was coincidently done at the peak of a few international data breach scandals. Users stated that the focus on privacy, control of data and security was excellent and that they were exited that such a tool, might be available in the future. Also, the linkage of the project to EU funding generated an additional goodwill for it.

With regards to usability, users recognized that for a prototype the ARIES app had a very good look & feel, and the design was good, despite some minor usability issues, that were in the meantime solved. It's important to state that later versions, including the current one, included a more intuitive and visual explanation of the different steps and was recognized to be good.

Finally, users mentioned that the need for a passport as a baseline for the user data was an interesting approach as this could generate additional trust in the system. It was often mentioned that the control of own's data in the ARIES vault was very important and that the cloud updates on the data being reflected in the third-party services was a huge plus. All in all, it was with no surprise that most users stated that they would likely use the service if it was available in the market.

11.5.2 Airport Scenario Pilot and Validation

The planning of the airport demonstrator began in January 2018 the work focused on refining the platform functionality and defining "use cases", with the planning of logistics and final storyboards following as time progressed over the summer and into autumn. Over a period of months this helped establish the approximate date where the development of the ARIES technology and the availability of the venue would be at its most optimum.

The venue of the demonstrator was a crucial and unique location. It held challenges in bringing an innovative concept prototype into a realistic operational environment. The location chosen was the Leeds/Bradford International Airport at Yeadon, in the City of Leeds, West Yorkshire, England. This location chosen for the demonstrator pilot, had far greater challenges to overcome than normal locations this was due to the secure nature of the site and the need to occupy the airport on airside, to perform an operational test on the ARIES prototype in a controlled access environment.

During the consultation stage with the airport, Jet2.com, Border force and a retail outlet, identified that the optimum time during 2018 for holding the pilot was the month of November. This was when the airport had the least flights and passengers in the terminal building, staff availability was at its most convenient and it would minimise the disruption to normal business in the airport.

The end users and stakeholders who took part in the pilot were identified during the consultation period. They came from the airport, airline, and retail sections of the airline experience. In addition to take into account law enforcement participants came from counter terrorism, cyber and serious organised crime officers with also a focus on crime prevention and community cohesion.

All participants were first asked to perform a timed exercise where they performed the ARIES enrolment process to establish an eID using their own genuine passport. During this process a live capture image of their face is part of the enrolment process. This is compared to the biometric information held in the passport and is a verification of identity. Multiple identities were enrolled on the devices and by way of a password, each person could secure their personal data on the device.

Once this had been completed each participant was given an additional enrolment exercise to complete to demonstrate some of the functionality of the ARIES app. These included a genuine expired passport. The date on the passport had expired, so no enrolment could be completed. With a forged passport which was very noticeable, the participants were unable to complete enrolment. Using a stolen passport which was genuine but where none of the biometric information matched the participant was also tried, so no enrolment could take place and no creation of an eID in ARIES.

The pilot was completed in one day and covered two main themed functions in the airport namely the passenger gate boarding process and a retail shopping experience. To help demonstrate and test the security of the facial recognition technology and to maintain participant's engagement, they were asked to try to pass the boarding process wearing various head garments;

this served to obstruct the live capture, since a clear image of the face is required for comparison. The final section in the boarding scenario was a timed exercise. Using the four devices all the passengers were asked to line up in a queue and were then timed on four separate occasions going through the boarding process. To best simulate a queue of passengers who all have their own mobile devices, the participants were organized in a pre-defined group and asked to queue, in order that they could be rotated four times using the four mobile devices in rotation. It is possible in ARIES to simulate each passenger having their own device, by creating multiple different user profiles on one device. Once all the participants had completed the exercise they were asked to complete a feedback questionnaire.

The second phase of the pilot took place in the retail store. A laptop was set up on the cashier's desk to simulate both the register's screen and the customer's screen. A walk though demonstration was first performed for the retail manager and staff. During the demonstration, the staff were shown how ARIES could be used to present the information they required to approve a sale of a restricted item, such as alcohol or cigarettes. They were asked to consider that using a recognized vID provider could be an approved method of proof of identity. It was also explained that one of the objectives of the ARIES project is to protect customers' personal information and not to disclose unnecessary information about the customer that could be stolen and used in a fraudulent act. From their own mobile device, the customer has to consent to releasing the above personal data for the Cashier to view. They were then asked to complete a questionnaire.

The feedback questionnaires contained a set of generic qualitative based questions about the user experience during enrolment. Further sub-sections in the questionnaire focused on questions bespoke to the stakeholders involved, i.e. the passengers and airline's boarding experience and retailer's and customer's purchase experience. The questions also aimed to explore exploitation and marketability, in terms of how likely passengers/customers would be to use the app if it were available and how likely a business would be to exploit a product like ARIES. Once all the storyboards and questionnaires were completed, a final opportunity was given to all participants to ask questions and give any feedback not already covered in the questionnaire.

The airport demonstrator was designed to explore the effectiveness of ARIES in issuing virtual credentials in an operational environment which requires the highest level of assurance and eligibility. The pilot demonstrated that a virtual identity combined with a live capture would greatly increase the security that protects citizens' and their credentials with assurances to service

providers and border officials, that the person is eligible to travel, or purchase items that are restricted by legislation.

The general performance of the prototype ARIES app and the verbal feedback given by participants, highlighted that the participants found the app easy to use and liked the concept of holding a duplicate electronic means of proving their identity; they also felt they were in control of that data.

Where ARIES failed to meet the KPI, was with the enrolment on the app; most participants commented that if they were enrolling at home rather than within a test environment, they would not have felt the pressure that came with performing the task in a timed session.

Comments from commercial end users focused on added security, reduced waiting times and efficiency savings in personnel. Comments also included the prospect of participants being able to spend more time in the commercial area of the airport, if the boarding process freed up waiting time. All participants saw clear benefits of the speedy boarding process; their customer experience in this stage of testing was very positive. While most users noted "some concern" in relation to concerns over privacy, no participants said they would not use the app. In fact, all users said if the app became a viable product, they would use it. Overall the pilot testing of the ARIES app was successful and the feedback useful and mostly positive.

11.6 Cyber-security and Privacy Research Challenges

The landscape of Identity Management (IDM) has been rapidly evolving since the effective launch of ARIES project in 2017. New identity management models have emerged, transcending the third party-based (identity provider) federated identity approach which has been dominating the identity and access management control landscape. In particular, multiple initiatives on Self-Sovereign Identity (SSI) are maturing and attracting attention from industry and governments [10].

These approaches are being supported on decentralised architectures enabled by Distributed Ledger Technologies (DLT) and more specifically Blockchain (noteworthy examples are Sovrin [11], Hyperledger Indy [14], uPort [12] or Blockstack [13]). Maturity of SSI solutions and widespread adoption has now a good basis on emerging international standards:

- W3C Credentials Community Group such as Decentralized Identifiers or DID [15]
- Decentralized Key Management System (DKMS) [16]

- DID Auth [17]
- Verifiable Credentials [18]

Furthermore, the European Commission contacted CEN/CLC, which has established a Focus Group on Blockchain and Distributed Ledger Technologies to collect identified European needs on these technologies, contextualised to Europe's specific normative and technological environment, monitoring relevant activities of the Joint Multi-Stakeholder Platform on ICT standardization and the Digitising European Industry initiative, while also supporting ISO/TC 307 with a possible future European Technical Committee on Blockchain and DLT, see [19].

The relevance of Law Enforcement Authorities for ARIES as key adopters engaged in the prevention and reduction of identity-related crimes, links well with analysed areas for use of Blockchain for Government and Public Services [20] and this points in the direction of more continuous development of ARIES sustainability when engaging with blockchain initiatives in the Public Sector, in particular, around the European Blockchain Forum/Observatory/Partnership [21] and future opportunities enabled by the development of a European Blockchain Services Infrastructure.

In this respect we can consider key technological breakthroughs achieved by ARIES and which define core features of its identity ecosystem which relate perfectly to major aspects required to materialise and achieve widespread adoption of the Self-Sovereign Identity paradigm:

1. ARIES implements a mobile wallet to manage derived identities, which is an essential client component in SSI approaches. This fully aligns with mobile identity orientation of ARIES, allowing full user-centric control of (user-owned) credentials and brings convenience and security to enrolment and authentication phases. In future phases, the ARIES app could also include an SSI Agent, acting as a trust anchor for establishing, by means of Agent-to-Agent Protocol, secure, authenticated connections to other agents (e.g. at relying parties). Coupled with DKMS protocol and Secure Element and Trusted Execution Element in mobile device, the wallet can maintain SSI private keys, extending use of these secure solutions already used for security of biometric material.
2. DID approach relates perfectly to ARIES approach of letting users manage multiple identities, bringing the additional advantage of allowing users to separate interactions and establish through DIDs encrypted channels with other entities (persons, organizations or things) to securely

exchange verifiable claims/credential data. This will allow to transition from an 'account-based' concept of IDM to based on user-managed connections over distributed blockchain solutions, with no central authorities that can be the target of attacks, thus achieving a more robust identity ecosystem.

3. ARIES derivation of reliable electronic identities from official or qualified credentials backed by the Member States (eIDASeID, ePassport) can be further explored, linking eIDAS network to ARIES provider for importing official identities into SSI infrastructure, see [22].
4. ARIES approach to data minimisation through Attribute Based Credentials, based on Zero Knowledge Proofs, aligns perfectly with the notion of SSI Verifiable Credentials, and allows once more, strict control by users of personal data disclosure with ease of use as cryptographic mechanisms ensure to relying parties that the user is in possession of certain attributes without revealing any additional unnecessary details, thus fulfilling GDPR data minimisation principle.
5. ARIES Secure Vault approach, with strict authorisation of access by users to competent identity crime investigation authorities, allows to explore in the future research possibilities to support this in private permissioned ledger technology, facilitating the cross-border investigation of identity related incidents and cooperation between Law Enforcerment Authorities.

All these aspects underline the readiness of ARIES results to reap opportunities, together with vibrant community of identity management experts, which are taking forward identity management ecosystems to a new paradigm of disintermediated and user-centric, privacy-respecting identity and access control. This will create clear benefits for the security of European citizens and organizations, helping authorities to collaboratively achieve EU strategic goals for identity fraud reduction.

11.7 Conclusion

As cyber-criminals evolve their cyber-attacks, the European Commission is determined to meet the challenge promoting research in different cybersecurity and privacy areas to mitigate upcoming identity-related crimes in both virtual (i.e. misuse of information, cyber-mobbing) and physical places (i.e. people trafficking, organized crime). In this sense, during the last years, research efforts in different projects has been made to devise novel solutions

aimed to increase user's privacy and protect them against evolving kind of cyber-crimes, the challenge is still ongoing.

To this aim, this chapter has summarized the main goals, challenges and the approach followed in European project H2020 ARIES project, whose ultimate goal is to provide security features that ensure highest levels of quality in secure credentials for highly secure and privacy-respecting physical and virtual identity management processes. In addition, the project has addressed key legal, ethical, socio-economic, technological and organisational aspects of identity-related crimes.

Novel processes such as virtual identity derivation, ACS, Id-proofings based on breeder documents, biometric process, along with security features (secure wallet, secure vaults) has been devised, implemented and validated for physical and virtual identity management, strengthening the link between physical-virtual identities to reduce identity fraud.

Acknowledgements

This book chapter received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700085 (ARIES project).

References

[1] The European Parliament, the Council of the European Union: Regulation (EU) no 910/2014 of the European parliament and of the council (2014).

[2] Hughes, J., Maler, E.: Security assertion markup language (saml) v2.0. Technical report, Organization for the Advancement of Structured Information Standards (2005).

[3] Hardt, D. (ed.): The oauth 2.0 authorization framework (2012).

[4] Camenisch, J., Van Herreweghen, E.: Design and implementation of the idemixanonymous credential system. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, pp. 21–30. ACM, New York (2002).

[5] Sabouri, A., Krontiris, I., Rannenberg, K.: Attribute-based credentials for trust (ABC4Trust). In: Fischer-Hübner, S., Katsikas, S., Quirchmayr, G. (eds.) TrustBus2012. LNCS, vol. 7449, pp. 218–219. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32287-721

[6] Kortuem, G., Kawsar, F., Fitton, D., Sundramoorthy, V.: Smart objects as buildingblocks for the internet of things. IEEE Internet Comput. 14(1), 44–51 (2010).
[7] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in Proc. Int. Conf. Secur. Commun. Netw., 2002, pp. 268–289.
[8] Jorge Bernal Bernabe, Jose L. Hernandez-Ramos, and Antonio F. Skarmeta Gomez, "Holistic Privacy-Preserving Identity Management System for the Internet of Things," Mobile Information Systems, vol. 2017, Article ID 6384186, 20 pages, 2017.
[9] J. L. C. Sanchez, J. Bernal Bernabe and A. F. Skarmeta, "Integration of Anonymous Credential Systems in IoT Constrained Environments," in *IEEE Access*, vol. 6, pp. 4767–4778, 2018. doi: 10.1109/ACCESS.2017.2788464
[10] European Blockchain Observatory, 'Blockchain innovation in Europe', https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf?width=1024&height=800&iframe=true
[11] Sovrin Foundation, https://sovrin.org/
[12] uPort, https://www.uport.me/
[13] Blockstack, https://blockstack.org/what-is-blockstack/
[14] Hyperledger Indy, https://www.hyperledger.org/projects/hyperledger-indy
[15] 'Decentralized Identifiers (DIDs) v0.11, Data Model and Syntaxes for Decentralized Identifiers (DIDs)', W3C Credentials Community Group Site: https://w3c-ccg.github.io/did-spec/
[16] DKMS, https://github.com/WebOfTrustInfo/rwot4-paris/blob/master/topics-and-advance-readings/ dkms-decentralized-key-mgmt-system.md
[17] 'Link to DID Auth final version', https://github.com/WebOfTrustInfo/rwot6-santabarbara/commit/c1c44d6d2ead845 db75f9a52b53c0fb4cd98db2d
[18] W3C. Verifiable Credentials Working Group, https://www.w3.org/2017/vc/WG/
[19] 'Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies", ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/ICT/ Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf
[20] European Blockchain Observatory 'Blockchain for Government and Public Services', https://www.eublockchainforum.eu/sites/default/files/

reports/eu_observatory _blockchain_in_government_services_v1_2018-12-07.pdf?width=1024&height= 800&iframe=true

[21] European Blockchain Forum and Observatory, https://www.eublockchainforum.eu/

[22] 'Importing National eID Attributes into a Decentralized IdM System', Abraham, A., June 2018,https://www.egiz.gv.at/files/projekte/2018/eIdAttributeImport/ ImportNationaleEIdAttribute.pdf