

Towards a Privacy-Preserving Reliable European Identity Ecosystem

Jorge Bernal Bernabe^{1(✉)}, Antonio Skarmeta¹, Nicolás Notario^{2(✉)},
Julien Bringer³, and Martin David⁴

¹ Department of Information and Communications Engineering,
Computer Science Faculty, University of Murcia, Murcia, Spain
{jorgebernal,skarmeta}@um.es

² Atos Research & Innovation Identity & Privacy Lab, Madrid, Spain
nicolas.notario@atos.net

³ Safran Identity & Security, Paris, France
julien.bringer@safrangroup.com

⁴ Gemalto, Integration & Consulting Services, Prague, Czech Republic
martin.david@gemalto.com

Abstract. This paper introduces the ARIES identity ecosystem aimed at setting up a reliable identity framework comprising new technologies, processes and security features that ensure highest levels of quality in secure credentials for highly secure and privacy-respecting physical and digital identity management processes. The identity ecosystem is being devised in the scope of ARIES European project and aspires to tangibly achieve a reduction in levels of identity fraud, theft, wrong identity and associated crimes and to create a decisive competitive advantage for Europe at a global level.

Keywords: Identity management · Privacy · Biometrics · Digital identities · Identity derivation · Secure wallet

1 Introduction

Personal data and, in particular, individual identities are getting more and more vulnerable in a digital world with European stakeholders interacting in globalized scenarios. This on-going and increasing lack of trust derives from the current deficiency of solutions, including consistently applied technologies and processes for trusted enrolment, identification and authentication processes, in particular the use of online credentials with low levels of authentication assurance. Furthermore, there is a lack of a coherent joint approach in Europe (in terms of legislation, cross-border cooperation and policy) to address identity-related crimes which costs companies, countries and citizens billions of Euros in fraud and theft, and which are quickly growing and serious crimes.

In this context, the ReliAble euRopean Identity EcoSystem (ARIES) H2020 European research project aims to provide means for stronger and more trusted

authentication, in a user-friendly and efficient manner and with full respect to data subject's rights for personal data protection and privacy. For that, it will include means to present a proof of identity without need to disclose more personal data than actually needed in a given interaction (data minimization and proportionality). The ecosystem will allow the citizen to generate a digital identity linked to the physical one using biometrics and at the same time to store enrolment information in a secure vault only accessible for law enforcement authorities in case of cybersecurity incidents [10]. This will allow linking proofs of identity based on the combination of biometric traits and citizen eID/ePassport with the administrative processes involved in the issuance of breeder documents (like birth/civil certificates).

Users will be also empowered with mechanisms that allow them to derive additional digital identities from the ones linked with their eIDs/ePassports, but with different levels of assurance and with different degrees of privacy about their attributes. These digital identities will be usable in administrative exchanges where it is required by the government according to eIDAS Regulation [16] and be stored in software or hardware secure environment their mobile or smart devices.

The rest of this paper is structured as follows. Section 2 describes identity theft and fraud and some of its challenges. Section 3 provides an overview of the ARIES ecosystem, including main components, features and interactions. Section 4 describes the main use cases addressed in ARIES, which allow to assess the feasibility and reliability of ARIES ecosystem. Finally, Sect. 5 concludes the paper.

2 Identify Fraud

Identity theft, according to sources such as the UK Home Office Identity Fraud Steering Committee or CIFAS, a fraud prevention organisation in the UK, is the obtention of information about an identity (e.g. name, date of birth, addresses) of another person. Furthermore, the usage of false or someone else's identity details for personal gain is what's considered **identity fraud**, which is one of the challenges to be addressed by the ARIES Identity Ecosystem.

Addressing identity theft is multi-dimensional problem and hence must be considered from different perspectives and involving multiple stakeholders. As an example, identity fraud can be prevented by improving user and document authentication technologies and processes making them more resilient. E.g. biometric checks could be included for high-risk transactions or for documents with high level of assurance. As biometrics are harder to fake, impostures will be limited. On the other hand, remediation mechanisms could focus on limiting the impact of such frauds by applying early-detection techniques or by facilitating the identification of fraudsters or impostors. It should also be considered a distinction between the legal or policy-related dimensions as opposed to the technological one. In the case of legal or policy, strong fines, identify theft reporting mechanisms can be established in order to discourage fraudsters.

A different perspective for identity fraud is related to the exact process of the identity management lifecycle where the fraud is targeted. Addressing identity fraud in the enrolment phase for the issuance of breeder documents requires strong biometric controls (e.g. fingerprint) and checking the authenticity of physical source documents. Meanwhile, the authentication phase may have different set of requirements such as detecting the user presence or to have multiple-factor authentication (e.g. eID and PIN number).

All these perspectives and dimensions must be considered in order to properly address more effectively the challenges posed by wrong identity, identity fraud and associated types of cyber and other forms of organized crime. One of the most challenging aspects of identity fraud is to somehow find the right balance of the three pillars of trust in physical and digital worlds: identity, security and privacy. Whenever stricter identity requirements are added, in general, more secure the system will be but, in exchange, privacy is usually diminished as additional personal data has to be disclosed. On the other hand, privacy-preserving (i.e. anonymous) systems, while fully legitimate, usually allows secondary malicious uses that are very challenging to avoid (e.g. bitcoins used to pay ransomware operators or anonymous social media accounts to make offensive comments).

ARIES will demonstrate how its ecosystem, based on eID digitizing, can avoid a trade-off between privacy and security and support both, in ways that enables the development of ethical apps acceptable to society. ARIES ecosystem's novel technical capabilities and procedures will relate breed documents with digital identities through citizen's biometrics, enabling the usage of strong mobile identities through a convenient and secure mobile identity wallet.

3 Related Work

Identity management is commonly addressed by using well-known technologies, such as the *Security Assertion Markup Language* (SAML) [9], OpenID [2], OAuth [8] or WS-Federation [17]. These technologies, are, in turn, used as baseline by most of the European research projects related with the ARIES EU project.

The STORK (2.0) [3] EU project establishes a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID/STORKs QAA model will shape the mobile identity derivation process. STORK's interoperability infrastructure is expected to be leveraged by ARIES components, which will might rely on STORK for certain kinds of eID authentications.

On the other hand, *Anonymous Credential systems* (ACS) [5] allow a selective disclosure of identity attributes to achieve a privacy-preserving identity management approach. A crucial aspect of privacy-preserving mechanisms is related to the design of mitigation strategies to avoid anonymity abuse, by considering *traceability* or *accountability* aspects. In this regard, ABC4Trust [14] EU project has provided advances for the federation and interchangeability of technologies supporting trustworthy and at the same time privacy-preserving Attribute-based Credentials. Nonetheless, ACS are still tacking off, mainly because of their

complexity and lack of user-friendly tools. In ARIES, privacy Attribute Based Credentials are being considered as a mechanism to support privacy-preserving identity management operations through user-friendly apps.

The FutureID [1] EU project built a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe. It is a holistic IdM that is able to interoperate with both, Abc4Trust and Stork technologies. Some FutureID outcomes are expected to be reused in ARIES to accomplish the goal of establishing a privacy-preserving and reliable European Identity ecosystem, which unlike in FutureID, it will support digital identity derivation.

The aforementioned EU projects do not allow to tie together trustworthy source documents with biometrical traits and derived mobile digital ID. ARIES will define a identity lifecycle processes to allow the linkage of physical identities and source breeder documents with new digital identities that can be derived from the physical ones, in order to maintain high levels of privacy preservation.

4 ARIES Identity Ecosystem

The main goal of the ARIES Identity Ecosystem is to provide new technologies, processes and security features that ensure highest levels of quality in secure credentials for highly secure and privacy-respecting physical and digital identity management with the specific aim to tangibly achieve a reduction in levels of identity fraud, theft, wrong identity and associated crimes and to create a decisive competitive advantage for Europe at a global level.

4.1 ARIES Ecosystem Overview

The process of authentication will be ensured with the use of a smart device allowing the acquisition of 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). These features will be obtained by functionality deployed either locally (on the smart device) or centrally (back-end). Digital identities will be generated with privacy preserving technologies and will allow citizens just to prove to be in possession of some attributes without exposing the rest of their data, i.e. being over 18 years of age. Given that different levels of assurance are possible a biometric mechanism could also be used as a proof of digital identity possession where appropriate [12].

Figure 1 shows an overview of the ARIES ecosystem, where interactions between the entities are depicted. The user manages several identities and credentials, which are issued by Identity Providers (IdP) and presented to the Service Providers (SP) to access the services offered 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

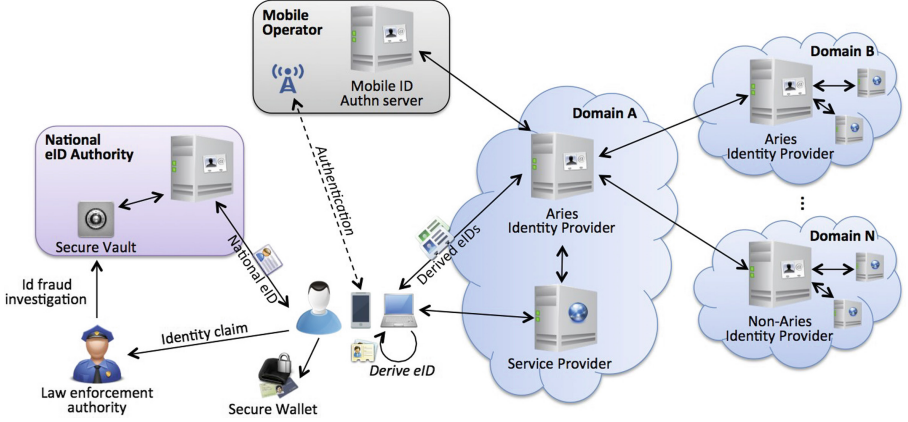


Fig. 1. Aries ecosystem

usually contains one or more IdPs and one or more SPs. The common use case is that a SP redirects user requests to the IdP within its own domain, although exceptions are also considered: a SP can directly authenticate the identity of the user (e.g. validating a certificate) and a SP could redirect to an IdP of another domain in which it trusts, including a mobile operator, a bank or a Government for Mobile eID authentication. 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 [9], OAuth2 [8], etc.

Users interact with the system through several devices, including computers and smart devices such as mobile phones or smart wearables. Such 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.

Users can request a new derived credential to an ARIES IdP after authenticating 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. For an IdP to issue a new identity credential, it should previously authenticate the user by requesting another credential that the user may already have and that should have been issued by a trusted IdP. Generation of derived credentials shall be logged to assure traceability to the real identity for law enforcement purposes. This could be achieved by an encrypted and signed

logging mechanism. This information should also be kept secured and only disclosed to law enforcement authorities in regulated cases.

In ARIES, the derived credential will be originated from existing strong credentials such as biometric data and a eID document. Namely, the credential derivation 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 a SP. In this case, identity approaches based on Zero Proof Knowledge like IBM Idemix [7] or ABC4Trust [14] solutions can be used. For this, the user should have previously obtained a special kind of credential, which is prepared with the needed cryptographic information to derive new identities and provide identity proofs when requested by a SP.

As identities can be derived and issued by different entities, each credential would have associated a Level of Assurance (LoA). This serves as a measure of the security mechanism used by the credential issuer to validate the identity of the user. ARIES aims to keep the LoA or to avoid significant differences when using derived credentials. Similarly, ARIES will try ensuring that Level of Trust (LoT) among different entities is also maintained after adopting derived credentials in the ecosystem.

Accessing a service supplied by a SP will impose some requirements for the credential to be presented, including providing attributes about user identity and trust requirements. The user can choose the mechanism and credential he want to present according to his preferences and the information and trust required by the SP. This includes the usage of a derived credential with less identity information and/or a pseudonym; 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 [11].

From the perspective of data protection, it is essential to take into account privacy by design principles, particularly 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) [15].

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 this aim, ARIES is devising 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.

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

Following, the most important individual concepts and actors that will conform the ecosystem are detailed.

4.2 Identity and Attribute Providers

Identity and attributes are not always differentiated in identity federation systems, however, for the purposes of ARIES and specially for its secure-and-privacy enhancing approach it is crucial to make a clear distinction between these two relying parties and their roles.

1. **Identity Providers** are a kind of service provider that provides subject authentication to other stakeholders within an identity ecosystem, such as service or attribute providers.
2. **Attribute Providers** are responsible for the processes related to the establishment and maintenance of the attributes associated to a subject. Attribute providers provides assertions of attributes to the individuals and other stakeholders, specially to service providers.

While in some standards, such as SAML [9], Identity Providers are responsible for provisioning the authentication and the attributes, there are two main reasons within the ARIES project for the separation of both concepts: (i) to support anonymous and pseudonyms interactions, in which the identity providers can provide an identifier which does not divulge any other personal data. (ii) Empower the user to choose different attribute sources that provide different sets of attributes with different levels of assurance. One of the requirements of ARIES project is to avoid the unnecessary linkage of attribute and identity providers with service providers, for which an identity wallet managed in the data subject's smartphone will mediate in between identity, attribute and service providers.

In any case, jointly, identity and attribute providers must establish and prove to relying parties who the subject is and to provide required information about the subject.

4.3 Secure Vault

The ARIES ecosystem relies particularly on the storage of identity evidence for ensuring the integrity of the identity digitalization, derivation and authentication

processes and for potential future investigation. This is implemented using a secure vault.

Secure vault technology is not new by itself and several products on the market are able to provide integrity, confidentiality, auditability and compliance with various security standards and legal requirements, to ensure that the content is safely stored, non-repudiation is enforced, and its authenticity can be legally assessed.

Nevertheless, ARIES emphasizes specific needs for securing e-ID documents and digital identities issuing process that justify the use of a secure identity vault at different stages of the architecture. The main motivation is storing the identity evidences used while proofing or authenticating an identity to generate a new digital ID. Following a privacy by design principle, the subject shall remain under control of his data. However, we foresee also the need for a legal authority to be able to access part of the content in case of identity fraud or cybercrime investigation.

ARIES will add additional features to modern secure vault technology to fully support the ecosystem processes. In particular, specific measures will be studied, such as proxy re-encryption [4], to avoid to handle cleartext data on the vault side, even when the requester of data is not the original provider. Some of the data will be accessible only to the subject. Some will be provided in case of legal investigation. And some non-sensitive attributes might be accessible to the system, where the vault will be able to play the bonus role of attributes provider (for instance to retrieve some attributes collected during the eID check, but not stored directly with the digital ID). Consent of the subject will be explicitly required for each attribute reading operation, except under legal authorization of authority investigation.

4.4 Digital Identity Derivation

New patented concept of identity and credential derivation is one of the starting points of ARIES ecosystem. The concept is based on creation of new anonymous credentials derived from existing strong credentials such as biometric data and a eID document. Newly created credentials, the ARIES token, should provide strong authentication means while preserving end user privacy. This credential derivation process is based on mobile token enrolment server with a derivation module.

4.5 Biometric Enrolment

The subject enrolment for issuing a digital identity relies on two important steps: validating he owns an established identity materialized with an eID document (more precisely an ePassport, a national eID or any kind of biometric electronic document issued by an authoritative source), and proving that he is the legitimate owner through biometrics authentication.

The main requirement is being able to ensure a good level of assurance while allowing self-registration on a smartphone. A mobile application will manage

digital and physical security checks of the eID: it will capture a biometric data of the subject, and while connected to a dedicated service, check both, authenticity of the chip inside the eID, consistency with the physical part of the document and the comparison of the biometric data with the reference biometric data in the chip will be verified. Thanks to the security features of the eID document and the additional use of anti-spoofing technology for biometric recognition, the process will provide high level of assurance.

Moreover, part of the validated data will be stored either on the secure vault or locally within a mobile wallet. Particularly, biometric data will be tied to some credentials in order to enable biometric authentication when using a digital identity (generated after the initial enrolment). To cope with privacy and security constraints, the biometric data will always be stored protected to avoid risk of leakage within non-secure places like the subject's smartphone or a web server, and comparison will be made exclusively on a secure environment.

4.6 Anonymous Credential Systems

Anonymous Credential Systems (ACS) [5], such as Idemix [7] or U-Prove [13] allow users to present Zero Knowledge cryptographic Proofs in order to prove possessing certain attributes in the credential. These systems enable a selective disclosure of identity attributes to achieve a privacy-preserving identity management approach. Indeed, a user can prove different predicates associated to a subset of identity attributes without disclosing the content of such attributes.

In ACS the credential *issuance* process allows a *Recipient* to obtain a credential from the Issuer. This credential consists of a set of attribute values, as well as cryptographic information that will allow credential's owner to create a proof of possession. The user acting as a *Prover* can demonstrate the possession of a certain credential to a SP (acting as a *Verifier*). Concretely, taking the example of Idemix, several zero-knowledge proofs are performed to convince the SP about the possession of such credential by making use of the CL signature scheme [6].

ARIES will try to introduce simple versions and adaptations of the ACS concept, deriving different digital partial identities over the whole original credential obtained from the ARIES IdP. The credentials will be maintained securely in the smartphone wallet to be used afterwards in certain scenarios that require different level of assurance. In addition, ARIES will try to provide user-friendly and privacy-preserving app for smartphones that will allow selective disclosure of attributes in an intuitive way.

5 Fraud Prevention

5.1 ARIES Enrolment and Authentication

After reviewing the current state of the art technologies, ARIES ecosystems incorporates a new flow of biometric enrolment of users and creation of ARIES tokens that would provide basic implementation of security and privacy requirements. The main goal is to create anonymous credential that may be used for

strong authentication and preserve a strong link between the new credential and biometric data that would allow examination of authorized parties for fraud investigation while preserving privacy.

The main use case of the ARIES project is user authentication. In the end, users should be able to use ARIES credentials to access online services or to be granted access to physical spaces. In order to acquire a new credential, users must enrol in the ecosystem using their smartphone.

In the first iteration of the ecosystem the privacy would be ensured by usage of anonymous identifiers and split of the data among many components so there would be no single point of failure that would allow disclosure of any personal data. While the first version of the ecosystem considers classical cryptographic schemes such as PKI and privacy based on process and deployment model, the second iteration is envisaged to be enriched by new schemes based on adaptations of Anonymous Credential Systems. In order to minimize privacy risks, ARIES ecosystem considers usage of ARIES Identity Provider for authentication of the tokens and a separate biometric Identity Provider for biometric enrolment and authentication. This would ensure the separation of ARIES data from the biometric information, improving privacy guarantees.

Enrolment. ARIES ecosystem enrolment process would with biometric enrolment; user's biometric data would be read and stored for future reference and his electronic document would be read to acquire his real identity. Note that the data would be stored in the secure vault that would enforce strong authorization process. At the end, the user would be given anonymous proofing ID that would be used for future reference to his biometric data.

After acquiring the proofing ID the user would be prompted to initiate creation of new ARIES token by scanning a QR code. During the enrolment, a new credential would be created in his ARIES application with anonymous ARIES ID that would be linked to his proofing ID in the ARIES Identity provider. At this step, the user may select which attributes would be provisioned to the token and provided to any relying party after successful ARIES authentication.

Authentication. The authentication use case is more similar to current state of the art cases because one of our goals is to provide smooth on-boarding of relying parties that use current SAML and OpenID Connect protocols. The main change will be in management of user information when the classical model will be replaced by privacy friendly scheme that would allow anonymous authentication while providing required attributes or proofs such as user age or state he comes from. The authentication would be managed by ARIES Identity provider application that would contact user's ARIES application and perform basic authentication. The result would be an anonymous ID and attributes provisioned with the credential. As an optional step, biometric authentication may be required.

5.2 e-Commerce Scenario

This use case aims to assess the specific challenges and difficulties in securing eCommerce transactions from identity fraud by including the technical robustness and security features of ARIES digital mobile identities in a realistic setting for provisioning eCommerce services. It also aims to assess the usability and convenience for customers of using ARIES digital mobile identities for both registration and authentication at the eCommerce online site. In addition, it will showcase more trustworthy interactions for citizens and customers with involvement of law enforcement stakeholders in the case of identity-related incident (using features of ARIES identity vault). This use case will compare the results with a ‘control’ environment in which the ARIES solution is not used in order to measure the positive impact of ARIES in reducing impact and levels of theft.

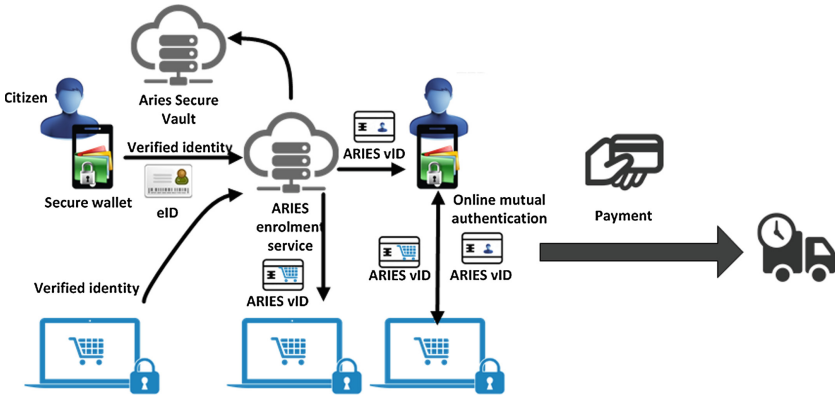


Fig. 2. Identity derivation components in the e-Commerce Use case

In order to address or prevent different identified identity theft use cases identified by law enforcement agencies, a typical eCommerce scenario has been re-designed to include ARIES technology (see Fig. 2):

1. Both, merchants and users must be enrolled in ARIES ecosystem by using digital certificates and eIDs which will provide them a digital identity;
2. Merchants will express through ARIES the minimum attributes, including required level of assurance, they require for customers' purchases. Customers will select the digital identity of their choice that meets merchants' requirements.
3. ARIES components at the eCommerce provider will check the validity of the digital identity and, if necessary, perform a biometric authentication (local or remote) using mobile device sensors (i.e. camera, microphone...).
4. Finally, and at the delivery stage, the recipient of the goods is also required to authenticate to the distributor, avoiding misappropriation of the delivered goods.

ARIES solutions are currently being developed. A first implementation of the ARIES ecosystem is expected to be validated for the e-Commerce scenario at the end of the first year of the project (September 2017), in Sonae, a multinational company with a diversified portfolio of businesses in retail, financial services, technology, shopping centers, telecommunications.

5.3 Identity Digitalization for Secure Travel Scenario

This use case 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.

As it is shown in Fig. 3, this use case contains two main process; obtaining the ARIES digital ID, and use the digital ID in the Airport scenario.

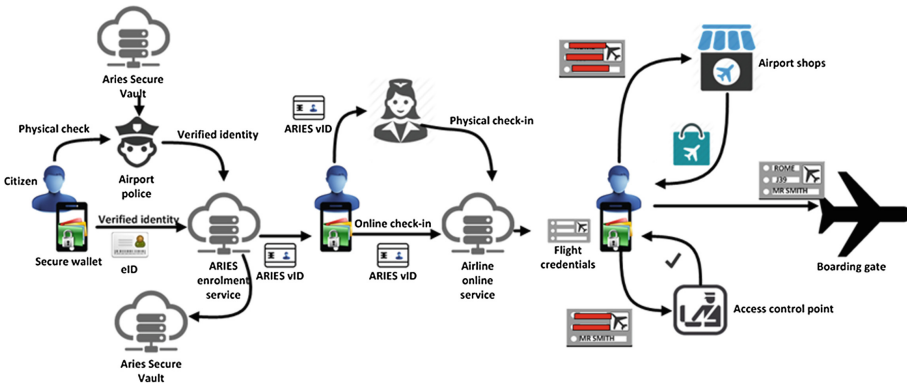


Fig. 3. Identity derivation components in the Airport Use case

Obtaining the ARIES digital ID:

1. The passenger self-enrols in the ARIES ecosystem by using her smartphone and eID/ePassport obtaining an ARIES vID linked to his eDocument.
2. Immediately, the passenger can present her mobile vID to obtain a boarding pass, linked to her mobile vID and to her biometric features and from which attributes can be disclosed in a privacy-preserving way. This credential will allow the passenger to go through airport's access control and board her flight.

Using the digital ID in the Airport scenario:

1. The passenger can demonstrate to the access control officers that she is allowed to go through the control by using her smart device and the recently issued digital identity to present a valid credential. No other information is disclosed except the minimum needed to compare with passengers list.

2. At the airport shop, the passenger can present an ARIES derived credential to provide a proof of ownership for a boarding pass to a flight outside the EU, without disclosing any additional information. This entitles the passenger to a VAT exemption.
3. The passenger at the boarding gate presents her smartphone and biometrically “unlocks” its ARIES derived boarding pass to access the plane.

The airport scenario is envisaged to be evaluated and validated during the second iteration of the project development (October 2018). In this sense, the ARIES ecosystem will be deployed and tested in a real airport (like the Brussels airport) and tested by a Law Agency Enforcement such as the Belgian Federal Police.

5.4 Supporting Law Enforcement Agencies

Law Enforcement Agencies (LEA) can be benefited from the ARIES technology as they might be granted to play the Inspector role in the ecosystem. The Inspector role is in charge of de-anonymize the user and access part of the data stored in the ARIES Security Vault, in case of identity fraud, misuse, liability or cybercrime investigation. To this aim, the Inspector should satisfy a policy that specifies which information should be recoverable as well as the inspection grounds describing the circumstances under the data can be inspected.

Notice that this authorization privilege is, in the end, materialized by endowing LEAs with specific cryptographic credentials that allow them decrypting such an information. Depending on the underneath technology, it might mean providing proxy re-encryption keys or anonymous credentials in case the LEAs need to access to Zero knowledge crypto proofs.

In ARIES scenarios LEAs can be granted to play the Inspector role in order to deal with identity fraud and identity tracking during the Airport Access Control. In the eCommerce scenario LEAs can take advantage of the ARIES capabilities to inspect payment transactions, thereby preventing refund fraud or fraudulent merchants.

6 Conclusions

ARIES European project is identifying, researching and testing the technological, organizational and societal means necessary to eventually establish the European electronic identity framework capable of addressing the challenges posed by wrong identity, identity fraud and associated types of cyber and other forms of organized crime. In this sense, this paper has introduced the identity ecosystem that is being currently devised and developed in the scope of ARIES European project. The ecosystem strives to safeguard the fundamental parameters of identity management: security, efficiency, user friendliness, trust, privacy and data protection. In the near future, ARIES will come out with an IdM architecture that will allow different kinds of credentials and mutual authentication mechanisms to provide the Level of Assurance required in each situation, enabling to

link the physical and digital identities in a secure and trustworthy way, while supporting data minimization techniques and anonymous credential solutions.

Acknowledgments. The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700085 (ARIES project).

References

1. Future-id, shaping the future of electronic identity. <http://www.futureid.eu/>
2. OpenID. <http://openid.net/>
3. Stork, Secure idenTity acRoss boRders linKed 2.0. <https://www.eid-stork2.eu>
4. Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 127–144. Springer, Heidelberg (1998). doi:[10.1007/BFb0054122](https://doi.org/10.1007/BFb0054122)
5. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001). doi:[10.1007/3-540-44987-6_7](https://doi.org/10.1007/3-540-44987-6_7)
6. Camenisch, J., Lysyanskaya, A.: A signature scheme with efficient protocols. In: Cimato, S., Persiano, G., Galdi, C. (eds.) SCN 2002. LNCS, vol. 2576, pp. 268–289. Springer, Heidelberg (2003). doi:[10.1007/3-540-36413-7_20](https://doi.org/10.1007/3-540-36413-7_20)
7. Camenisch, J., Van Herreweghen, E.: Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, pp. 21–30. ACM, New York (2002)
8. Hardt, D. (ed.): The oauth 2.0 authorization framework (2012)
9. Hughes, J., Maler, E.: Security assertion markup language (saml) v2.0. Technical report, Organization for the Advancement of Structured Information Standards (2005)
10. Naumann, I., Hogben, G., et al.: Privacy features of european eid card specifications. Technical report, The European Union Agency for Network and Information Security (ENISA) (2009)
11. Kortuem, G., Kawsar, F., Fitton, D., Sundramoorthy, V.: Smart objects as building blocks for the internet of things. *IEEE Internet Comput.* **14**(1), 44–51 (2010)
12. Li, S., Kot, A.C.: Fingerprint combination for privacy protection. *IEEE Trans. Inform. Forensics Secur.* **8**(2), 350–360 (2013)
13. Paquin, C., Zaverucha, G.: U-prove cryptographic specification v1. 1. Technical report, Microsoft Technical report (2011). <http://connect.microsoft.com/site1188>
14. Sabouri, A., Krontiris, I., Rannenberg, K.: Attribute-based credentials for trust (ABC4Trust). In: Fischer-Hübner, S., Katsikas, S., Quirchmayr, G. (eds.) TrustBus 2012. LNCS, vol. 7449, pp. 218–219. Springer, Heidelberg (2012). doi:[10.1007/978-3-642-32287-7_21](https://doi.org/10.1007/978-3-642-32287-7_21)

15. Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., Oliveira, A.: Smart cities and the future internet: towards cooperation frameworks for open innovation. In: Domingue, J., et al. (eds.) FIA 2011. LNCS, vol. 6656, pp. 431–446. Springer, Heidelberg (2011). doi:[10.1007/978-3-642-20898-0_31](https://doi.org/10.1007/978-3-642-20898-0_31)
16. The European Parliament, the Council of the European Union: Regulation (EU) no 910/2014 of the European parliament and of the council (2014)
17. Weerawarana, S., Curbera, F., Leymann, F., Storey, T., Ferguson, D.F.: Web services platform architecture: SOAP, WSDL, WS-policy, WS-addressing, WS-BPEL. WS-reliable messaging and more, Prentice Hall PTR (2005)

Privacy Technologies and Policy

5th Annual Privacy Forum, APF 2017, Vienna, Austria,

June 7-8, 2017, Revised Selected Papers

Schweighofer, E.; Leitold, H.; Mitrakas, A.; Rannenberg,
K. (Eds.)

2017, XIV, 231 p. 59 illus., Softcover

ISBN: 978-3-319-67279-3