ARIES: Evaluation of a Reliable and Privacy-preserving European Identity Management Framework

Jorge Bernal Bernabe[a], Martin David[b], Rafael Torres Moreno[a], Javier Presa Cordero[c], Sébastien Bahloul[d], Antonio Skarmeta[a]

[a] *University of Murcia, Spain*
[b] *Gemalto, Czech Republic*
[c] *Atos Research, Spain*
[d] *IDEMIA, France*

Abstract

Despite several efforts in the last years to make Identity Management Systems (IdMs) reliable, secured and privacy-respectful, identity-related cybercrimes are still continuously expanding. Current IdMs lack of proper security and privacy mechanisms that can holistically manage user's privacy, strong authentication and ID-proofing mechanisms based on biometrics, usage of breeder documents, while maintaining usability for mobile, online or face-to-face scenarios. To fill this gap, the ARIES EU project aims to set up a reliable identity ecosystem, combining mature technologies for meet highest level of assurance, such as biometrics or use of secure elements, with innovative credential derivation mechanisms. ARIES has devised and implemented a privacy-preserving and user-centric Identity Management framework as well as associated management practices that ensure usability and flexibility for identity management processes. This paper presents ARIES results obtained after the successful development and validation of the ARIES IdM System in the associated use cases.

Keywords: Privacy, security, risk reduction, identity management systems, identification, biometrics, virtual identities, identity derivation, secure wallet

1. Introduction

Identity theft or forgery and related cyber crimes are continuously evolving. With growing value provided by online services the cyber criminals explore new attack patterns and improve their techniques. The scale of cyber fraud challenges both resources and technical mechanisms of online companies, governments and Law Enforcement Authorities; new attack paths require innovations of existing solutions and new approaches to strengthen security and privacy of the end users. In addition, mobile communications are increasing the solution landscape, opening additional attack surface for mobile malware and rouge apps [1]. Usual online attacks such as phishing and impersonation can exploit vulnerabilities of additional devices and with new Smartphone use cases the threats may newly target both online and face to face scenarios.

However, there is a lack of reliable and privacy-preserving self-sovereign Identity Management Systems (IdMs) that would empower users with full control over their identities in diverse scenarios while addressing identity related threats. In this sense, there is a need for IdM system addressing the identity management in a holistic way, encompassing: identity proofing, identity derivation, strong multi-factor authentication based on biometrics, privacy-preserving attribute proving, as well as supporting cyber-crime prevention and incident investigation. In addition existing Mobile Identity solutions lack assurance mechanisms based on identity derivation from official physical breeder documents (ePassport and National's eIDs) that would provide sufficient trust.

Email addresses: `jorgebernal@um.es` (Jorge Bernal Bernabe), `martin.david@gemalto.com` (Martin David), `rtorres@um.es` (Rafael Torres Moreno), `javier.presa@atos.net` (Javier Presa Cordero), `sebastien.bahloul@idemia.com` (Sébastien Bahloul), `skarmeta@um.es` (Antonio Skarmeta)

To fill this gap, Aries (ReliAble euRopean Identity EcoSystem)[1] European project has implemented a holistic identity management system that meets those characteristics. The aim is to address the aforementioned issues, from the very beginning. To design, develop and evaluate an identity management framework that has been specially tailored for reduction of identity fraud, improving the security in the management of personal identity data, in online, mobile and face to face scenarios. The system prevents identity impersonation and helps to preserve user privacy through innovative mechanisms and biometric techniques. It strengthens link between physical identity (based on breeder document such a ePasport) and derived digital identity (MobileID and mobile anonymous credentials), in order to mitigate identity-related threats. In addition, ARIES provides new identity and activity inspection options for Law Enforcement Authorities (LEAs) under strict access control fully in hands of the user, while the data are stored in a secure component protected by anonymization and encryption.

Aries IdM framework has been successfully deployed, validated and tested in two main Pilots. The first one is related to online eCommerce transactions that requires strong authentication and high level of assurance and trust using face recognition techniques with mobiles, whereas the second scenario is intended to reinforce the current face-to-face identity management processes, such as airport user journey. The airport scenario demonstrates the Aries capabilities to replace physical eIDs with mobiles in certain processes, for instance allowing self-boarding in the plane with the highest Level of Assurance using dedicated boarding cameras, combining face recognition and mobile PKIs technologies with virtual identities originally derived from official physical eIDs. It also shows the capabilities to strengthen user's privacy revealing the minimal amount of personal information (e.g. demonstrating certain predicates over personal attributes using Zero Knowledge Proofs [2]) in face-to-face digital purchases inside the airport, through the Aries App.

The main contributions of Aries, described in this paper, are manifold:

- Firstly, this paper details the Aries framework design, which has managed to integrate the latest privacy-preserving solutions based on Anonymous Credentials Systems (ACS), identity proofing and derivation-methods using physical breeder eID documents, authentication and Biometric techniques that protect against impersonation attacks, LEAs investigation procedures, while following a user-centric approach, using mobiles, to keep usability levels.

- Secondly, the paper describes the implementation of the Aries IdM framework, that has been fully developed and deployed in diverse scenarios using mobiles, either face-to-face (authentication in airports) or online (eCommerce), showing its capabilities for adapting to diverse Biometric techniques (face and voice recognition), eIDs (ePassports and spanish eID), authentication methods (Anonymous-based credentials, Mobile PKI solution).

- Lastly, this paper provides the empirical performance evaluation of the Aries IdM platform with the aim of assessing the feasibility, efficiency and reliability of the system. The paper also shows the successful user's acceptance evaluation results. The obtained results demonstrate the Aries's benefits: to strengthen the security and trust in identity-related processes while maintaining user-friendliness and usability aspects, increase user's privacy, reduce and prevent identity fraud.

The rest of this paper is structured as follows. Section II describes the state of the art in the research field. Section III is devoted to the explanation of the ARIES identity management framework, including their main identity management processes. Section IV describes the implementation in the two main scenarios developed and tested in ARIES. Section V delves into the performance evaluation and security analysis of the framework. Finally, Section VI concludes the paper.

2. Related Work

2.1. State of the art in Identity Management and privacy

Traditional identity management technologies, such as SAML[3], OpenID [4], OAuth [5], provide security and privacy solutions in federated online scenarios [6]. *Anonymous Credential systems* (ACS) [2] like Idemix [7] allow minimal disclosure of personal attributes enabling privacy by design features to the identity management system.

[1] Aries (ReliAble euRopean Identity EcoSystem). H2020 EU Project, Grant Agreement No 700085. `https://www.aries-project.eu/`

ACS rely on Attribute-based credentials and cryptography operations, such as Zero-knowledge crypto-proofs (ZKP), to provide pseudonymity, anonymity and minimal disclosure of attributes with diverse predicates. Nonetheless, ACS are still not widely used for their complexity and lack of user-friendly tools.

ACS have great potential and applications. Indeed, they are being considered in innovative computing scenarios like in Blockchain [8] to democratize the identity management, and in Internet of Things environments [9] [10] to deal with the privacy of Smart Object's identities. However, ACS has not been yet addressed properly in end user mobile scenarios and in scenarios utilizing attribute credential derivation from user's breeder documents. This would enable a self-sovereign and privacy-preserving identity management model, where users can have full control of their personal information in their smartphone. Recently Gunasinghe et al. research proposal [11] defines a biometrics-Based authentication protocol from Mobile Phones employing ZKPs. Indeed, ZKPs are being explored for privacy-preserving Identity and personal data management in diverse novel distributed technologies like blockchain [12].

Other advanced authentication and privacy-preserving mechanisms are currently starting to get research attraction. In this regard, Camenisch et al. [13] propose a threshold-based cryptography approach to verify passwords in an optimal distributed way to increase security against one unique Identity Provider. Likewise, the PASTA protocol introduced by S.Agrawal et al. [14] introduces a novel threshold-based authentication. However, these technologies are not providing fully unlinkability and therefore the use of other cryptographic technologies such as blind signatures, can be used as another step forward on top of PASTA in the privacy management. Following this line, [15] introduces a new privacy-preserving framework, using novel crypto-privacy mechanisms o top of the above mentioned techniques, to split up the role of the online IDP over multiple authorities, so that no single authority can impersonate or track its users. However, the aforementioned research works, unlike in the ARIES solution presented herein, are not intended to integrate ID-Proofing based on biometrics and breeder documents as part of the IdM.

2.2. State of the art in Authentication, Biometrics and eID derivation methods

Biometric authentication systems allows recognition of an individual by taking into account his biological and/or behavioral features. The main advantage of biometrics is that they are unique and personal, enabling strong authentication. On the other hand, these characteristics are permanent and can not be renewed, therefore the process itself need to be properly handled to avoid biometric data leakage either in-transit or at rest when stored in the Service Provider (SP). In this sense, Ratha et al [16] outlined advantages and power of biometrics-based authentication, recognizing weak spots that may impose potential security threats.

Recently, [17] has studied five key factors that lead to success of a biometric system in a context of financial services, analyzed challenges and trends that need to be considered. A complete review of state of the art in biometric technology and recognition techniques can be found at [18]. Kindt et al.[19] described risks when using Biometrics for identification of citizens. In this sense, regarding the face recognition, latest techniques, like the one proposed in ARIES, incorporates Attack Detection Methods for counter-spoofing [20] [21] uses hybrid software-based approaches, that consider different techniques such as optical flows, movement magnification or the usage of invariants 3D Objects to detect spoofing attacks. Moreover, current trend in Biometric management systems is to avoid storage of biometric information on the server side, and integrate public-key cryptography for authentication, as it is specified by the FIDO UAF (Universal Authentication Framework) [22]. As in Aries, FIDO allows handling local authentication requests and communicate with a server for remote verification. However, unlike Aries, FIDO is not intended to support vID creation and derivation based on eID breeder documents such as ePassport.

Regarding identity derivation and linkage of physical and virtual identities, authors in [23] analyze how the eID, and concretely ePassport, can be used as a breeder document for Identity Management. ARIES deals with the whole life-cycle of identity, defining mechanisms to link physical identities and source breeder documents with new digital identities derived from the documents and provides a reliable Identity management solution with high level of assurance and privacy preservation.

The first introduction of ARIES ecosystem was presented in [24], however, by that time, ARIES was just starting and most of the architectural designs were at its early stages. This paper describes the architecture devised to provide a reliable and privacy-preserving European identity ecosystem, intended to cope with the vast majority of identity-related use cases for smartphones based on biometrics and eID, either face to face (e.g. airport boarding) or remote (e.g. e-commerce purchase).

3. Aries IdM Framework Design

The Aries IdM system presented herein has two main technical requirements: privacy by design and possibility to provide information to LEA under well defined conditions. Current multi-modal authentication solutions are usually a result of long ongoing process when new features are added to existing system rather than solutions built from the scratch. The process is usually an introduction of a new feature for few pilot users when full backward compatibility is kept for all users and phase-out period when the deprecated features are dropped and old users using them are notified to migrate the new ones. This is typically a process followed by banks when user acceptance is as important as security. In this sense, ARIES is intended to be adopted by existing enterprises trying to improve existing solution with gradual changes rather than newly built solution following all recommendations from the beginning.

Literature review indicates that there is a limit of privacy that an IdM solution may achieve, when the privacy aspects are not considered from the early beginning, or if the solution reuses existing bricks not preserving the privacy. Thus, privacy by design has been built into the design of ARIES components. Besides, segregation of duties must be kept when existing components are reused to limit impact of possible privacy compromise.

The possibility to investigate incidents by independent entities is also a new feature usually not included as a technical requirement in most of the existing solutions. State of the art technologies usually either provide standard audit log trail that may compromise privacy of the user or limit the logging to the degree the preserved information does not contain much usable information. ARIES IdM has been designed in cooperation with LEA representatives to provide a framework definition usable also as a guideline for similar systems in future. Apart from the usual inspection of user's hardware which is not related to ARIES, the LEA uses audit log with full information (time, credential used, IP address, time) to enable cyber-crime investigation. However, the audit log with such information would be a severe threat to user's privacy, so that it must be stored securely and the control over the data should be fully in hands of the user, even though this partially limits the investigation possibilities in case the attacker creates virtual ID using forged document.

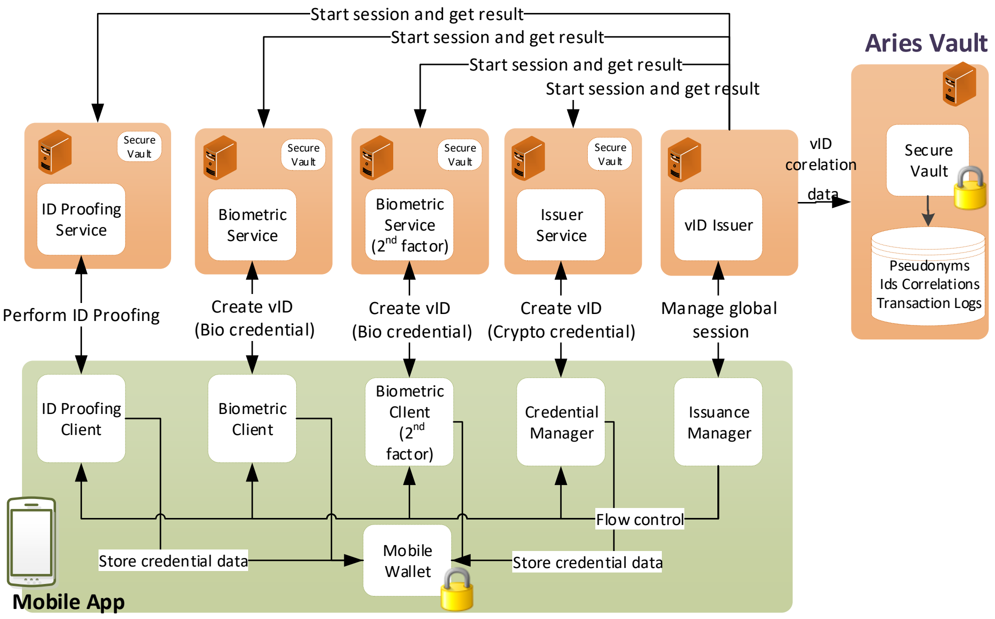


Figure 1: Issuance architecture

The Aries IdM functionality can be split in two main processes, i.e. Identity Issuance and Authentication. Regarding the Issuance, Figure 1 shows the Aries IdM Issuance architecture. The user's virtual identity is build in different steps: ID Proofing, enrolment of one or more features for biometric authentication and creation of credentials for Aries authentication. The information collected during the creation process must be bound together to make sure it is linked to same virtual ID. At the same time the information retention must be minimal to follow privacy by design approach. In order to minimize data retention the architecture utilizes user's App as a storage of intermediate products.

The requirements imply that there should be one component working as a boiler plate and orchestrator of the issuance process: Issuance manager. The component is responsible for starting and finishing the process and order of the steps in the session and to preserve information about which components were used during the creation process. It does not collect or process any user information only the result of the process. All the steps are executed by their respective server side components and corresponding SDK modules in the App. Each step starts with a back-end call to initiate the step body and to open session. The step body consists of vendor proprietary communication and result is always an identity part reference (anonymous id). Once the step is finished the App notifies the Issuance manager and it contacts the back-end to verify the step session has been finished successfully and the identity reference is valid for the session. Once the process has ended the Issuance manager stores all the identity references to be able to resolve the links during the authentication process.

On the other hand, Figure 2 shows the Aries IdM authentication architecture that follows the same Issuance pattern. The identity verifier provides OpenID Connect authentication interface for service providers and works as an orchestrator of the flow, steps are implemented by vendor components. In the simplest deployment model the application may also perform verification of Aries credentials. Selection of the flow steps is based on available features and authentication strength requested by the service provider.

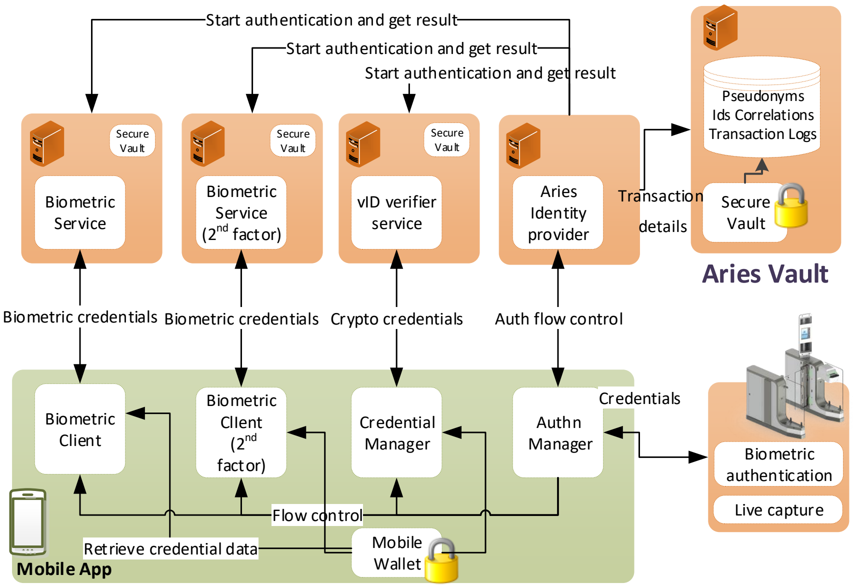


Figure 2: Authentication architecture

The rest of this section describes the main Aries IdM processes, encompassing, ID-Proofing, Biometric enrolment, vID Issuance, Authentication (including Biometric authentication and privacy-preserving authentication) and Law Enforcement Investigation.

3.1. ID-Proofing process

3.1.1. ICAO ID proofing

The ID proofing workflow integrated within ARIES is as follows. Firstly, the document front is captured on the device. Then, an optical character recognition of the Machine Readable Zone (MRZ) is processed. Afterwards, using the MRZ information, the key to get the contact-less access to the document is computed. The electronic version of the data are retrieved and sent to the IPV server. Finally, the IPV server checks the data and portrait signature according to the country that has issued the passport.

In order to demonstrate that the passport is a fresh copy, and depending on the portrait capabilities active or passive authentication is done, this is, Basic Access Control (BAC) or Extended Access Control (EAC) are employed as described by ICAO (International Civil Aviation Organization) [25]. Thus, the server generates the challenge that has to be signed if possible. In the ARIES IPV integration, the data are sent back and forth between the server and the mobile device. Without implementing this approach, the data could be registered and replayed performing an impersonation of the user.

3.1.2. Spanish eID proofing

In order to provide an eID proofing based on different document than ePassport, a component is developed in Aries using the official National Document of Identification. In the implementation the eID is the official Spanish eID, namely DNIe v3.0. Therefore, this component provides ID proofing based on the personal information stored in the DNIe.

To obtain the personal data from the chip of the document is necessary, firstly, using the camera of the mobile device to read the MRZ characters printed on the bottom of the back face of the document. With these characters it is able to obtain the necessary access key to open a secure NFC channel between the mobile device and the physical smart card. Then, a library (jMRTD in current Aries implementation) enables the device, under the Basic Access Control (BAC) protocol, to obtain the required digitally stored information from the chip of eID document. The chip generates and sends a random number to the antenna of mobile device, then mobile device encrypts the number using the access key obtained and transmits it back to the chip. This way, the chip could check if the number has been encrypted with the right access key and allows the mobile device to access the digital data. The complete workflow of this proofing module can be simplified in these three first steps, secondly the signing process of mentioned information using JSON Web Token (JWT) standard for this purpose, finally, sending everything packaged to the ID proofing module where the information extracted will be used for next task, namely biometric enrollment, performing a comparison of the data from the chip and live data to verify the identity.

3.2. Biometric Enrollment

This step is required as the ARIES ecosystem has been designed as a multi-vendor platform. After identity verification, a biometric registration should be conducted. At the moment, two modalities are supported: the portrait and the voice, explained below.

3.2.1. Facial Enrollment

For facial authentication, the initial enrolment has already be done by the government with ICAO compliance criteria. During ARIES enrolment the portrait image is retrieved in the IPV to be matched with the document holder, so a first facial biometric matching is done at that moment.

The needs of a biometric enrolment component are multiple:

- *Interoperabilty*: Images are the only inter-operable format that can be used by the architecture between the different components - facial biometric template formats being vendor proprietary. In ARIES the components to be considered are the Identity Proofing and Verification on one side, and the facial matching component taking care of enrolment and authentication on the other. In the design, the architecture ensures that the portrait enrolled in one component could then be later reused in the other.

- *Performance*: As biometric coding is an expensive task (comparing to matching), thus the authentication relies upon a matching between a onetime coded reference template and the live capture.

- *Privacy protection*: Instead of manipulating the biometric data (here the template) in a clear format, one of the operation done during the enrolment is encryption. Therefore, even if the data is stolen on the device, it cannot be used.

The data are collected on the mobile, sent to the server, processed on the server for eligibility and quality checks but not stored on server side for later authentication. The biometric data are associated with anonymous identifier only. The Biometric service does not have access to previously obtained information from electronic document. Once processed on the server is finished, the biometric template is encapsulated in a biometric token, that is signed and encrypted by the biometric service, and sent back to the mobile for storage. Therefore, there is no storage of biometric data at rest in server-side.

3.2.2. Voice Enrollment

The voice enrolment, uses samples that consider English spoken numbers, the enrolment process considers at least three sets of three numbers, more samples may be requested if the quality is not up to expectation, the authentication considers three samples with limited repetition in case of retry. The service was originally designed for help desk authentication by phone, and so that the API is adapted for is integration in Aries.

The original service architecture considers the functionality on the server side only, the client is thin, it only collects the voice samples, encodes them and sends them for verification. This on one hand simplified App development, but on the other hand has impact on amount of data transmitted and on user experience. In integration the voice enrolment is added as an option of enrolment flow and to simplify the implementation the choice is delegated to the user. In the App the user has a possibility to do the voice authentication step after the original face enrolment or it may be skipped and follow the nominal ARIES flow.

Voice authentication is implemented using existing service by Polygon[2]. The integration was based on a thin proxy between ARIES components and existing backend Polygon service. The original service was a set of typical http endpoints, but it also required usage of cookies for session management which was not aligned with pure REST ARIES architecture, so the main task of the proxy was to manage the cookies, move session management to specific parameter and to provide REST endpoints with same flavour as other ARIES enrolment services.

The implementation does not store any information in the mobile App and all biometric information for voice recognition is stored on server. This is in clear contrary to the ARIES requirement that all information must be in control of the user and no biometric information should be persisted by the server. This is accepted as clear goal of the integration is to demonstrate the architecture is flexible and existing services may be used by ARIES at small cost. It must be noted that server side information contains only an anonymous user reference so also in this case the basic segregation of duties provides protection against most of the usual threats such as database theft.

In order to achieve fully ARIES compliant production same pattern as in case of face verification is employed. The data is processed by the server, tokenized and pushed to the App. This option strongly depends on the verification technique used and may be difficult for implementations using pure machine learning.

In case the underlying service can be modified then the implementation should also take into account user experience during system design phase. The implemented flow has been limited by API capabilities and could be considered slow and hard to use. Partial data processing in the client would be recommended to allow fast local rejection of low quality samples or samples with too much background noise. The preprocessing should involve at least basic audio data compression to lower amount of information sent over network.

3.3. vID Issuance

Issuance flow, described in Figure 3, starts with device capabilities negotiation with the Issuance manager. This is an optional step that allows optimal choice of features and backend service instances if the solution uses multiple instances of any of the services. ID Proofing is done as a next step and may be combined with enrolment of biometric features, if the features may be read from the electronic document. Additional biometric features are enrolled as independent credentials in any number of steps to support multimodal authentication. Once the biometric enrolment has been finished the Issuance manager triggers creation of cryptographic credential used for Aries authentication.

Virtual Identity issuance step 3 is the last step of the user and must result in creation of a new credential linked to the information obtained during the previous steps. Aries architecture does not define the type of the credential or how the credential is created. This is left up to each implementation.

Pilot implementation selected Mobile PKI credentials as the main technology for pilot user tests and Anonymous Credential System to demonstrate the architecture may accommodate innovative credential technologies.

[2] Polygon https://polygon.pt/

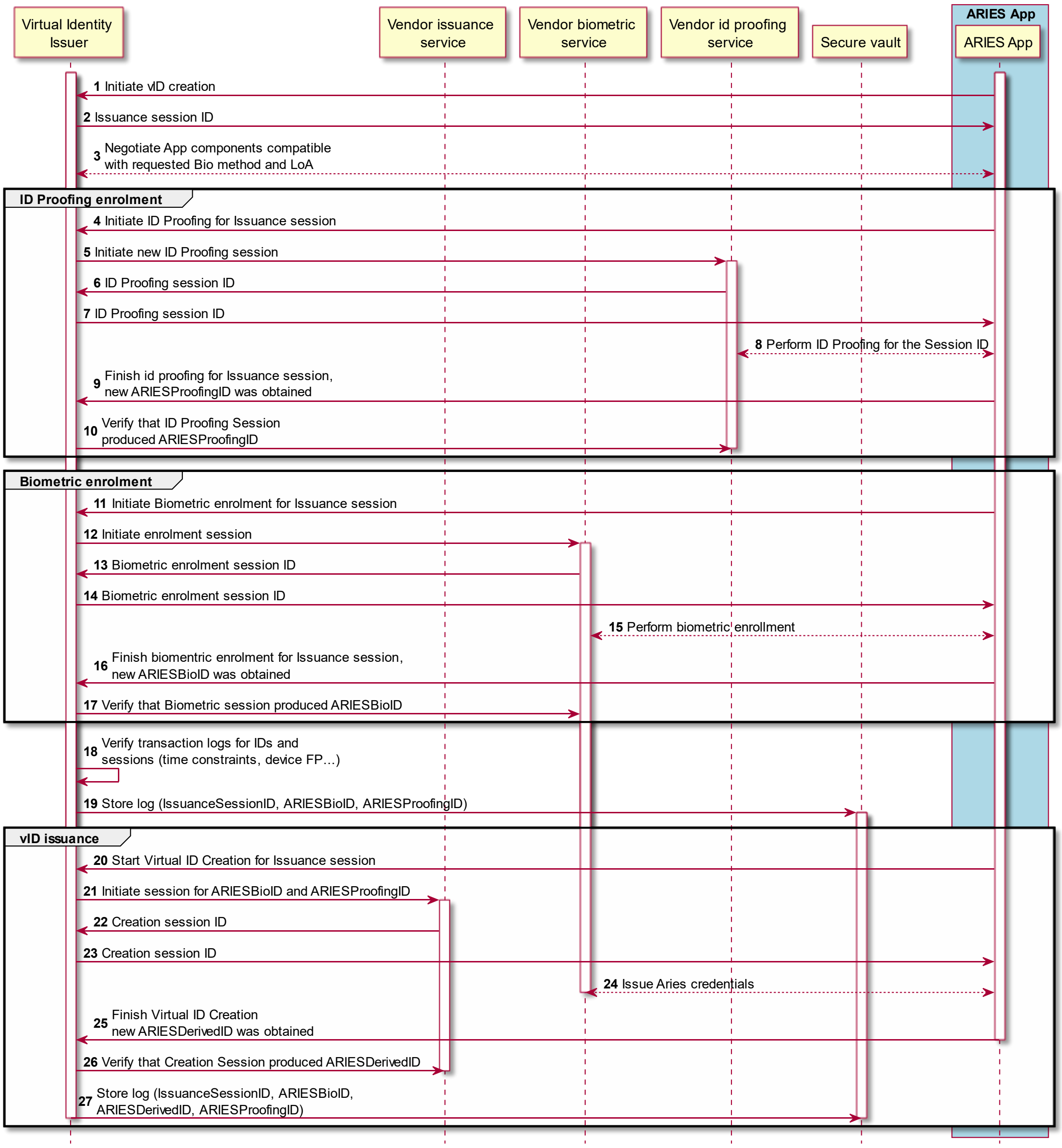

Virtual Identity Issuer
Vendor issuance service
Vendor biometric service
Vendor id proofing service
Secure vault
ARIES App
ARIES App
1 Initiate vID creation
2 Issuance session ID
3 Negotiate App components compatible with requested Bio method and LoA
ID Proofing enrolment
4 Initiate ID Proofing for Issuance session
5 Initiate new ID Proofing session
6 ID Proofing session ID
7 ID Proofing session ID
8 Perform ID Proofing for the Session ID
9 Finish id proofing for Issuance session, new ARIESProofingID was obtained
10 Verify that ID Proofing Session produced ARIESProofingID
Biometric enrolment
11 Initiate Biometric enrolment for Issuance session
12 Initiate enrolment session
13 Biometric enrolment session ID
14 Biometric enrolment session ID
15 Perform biometric enrollment
16 Finish biomentric enrolment for Issuance session, new ARIESBioID was obtained
17 Verify that Biometric session produced ARIESBioID
18 Verify transaction logs for IDs and sessions (time constraints, device FP...)
19 Store log (IssuanceSessionID, ARIESBioID, ARIESProofingID)
vID issuance
20 Start Virtual ID Creation for Issuance session
21 Initiate session for ARIESBioID and ARIESProofingID
22 Creation session ID
23 Creation session ID
24 Issue Aries credentials
25 Finish Virtual ID Creation new ARIESDerivedID was obtained
26 Verify that Creation Session produced ARIESDerivedID
27 Store log (IssuanceSessionID, ARIESBioID, ARIESDerivedID, ARIESProofingID)

Figure 3: Issuance process flow

3.3.1. Mobile PKI

Usage of PKI in mobile authenticators is considered current state of the art. The PKI based authenticators usually provide digital signature capabilities on top of the authentication and acceptance of the solution usually depends on certificate issuance process. In most of the cases the authentication also provides user identification: the certificate is unambiguously linked to real person identity. PKI based solution has been selected to provide an example of implementation that is improvement of current systems and may utilize applications available on the market.

Aries PKI authenticator is based x509 specifications and in order to provide required anonymity each identity created consisted of a X509 certificate containing a random identifier and a set attribute certificates each containing a single user attribute.

3.3.2. Anonymous Credential System Issuance

The issuance process is a two-round interaction where the User submits a request containing his attributes and the Issuer certifies the fact that the User has the claimed attributes by returning the credential that is stored in the user wallet.

The issuance process is carried out through Idemix, Figure 4. Issuance of Idemix credential is done on user request, not during the enrolment flow, and it uses previously obtained information from ID Proofing. This process follows the same pattern as other Aries enrolment steps.

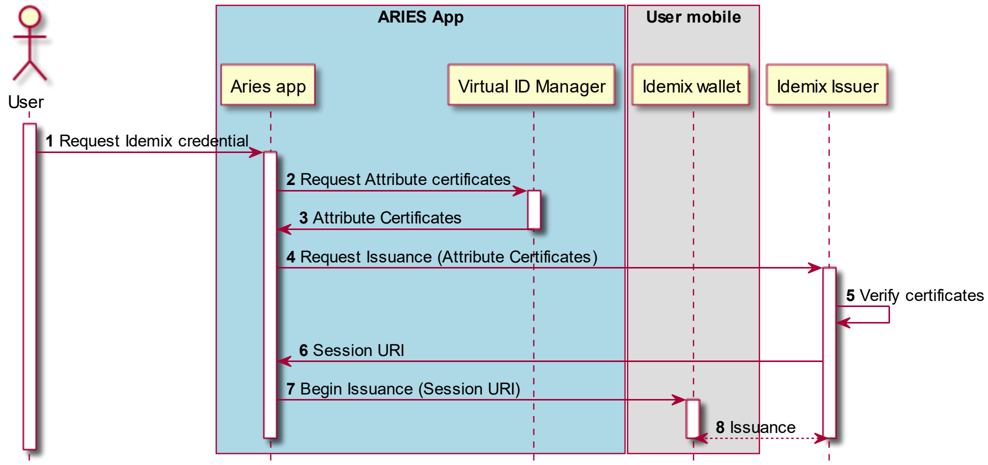


Figure 4: Idemix Identity Issuance in Aries

Step 8 in Figure 4 performs the Idemix issuance protocol [26] between the subject or recipient (Aries user mobile) and the Idemix issuer (part of the IdP). The Idemix issuance process is summarized in the following steps:

- Firstly, the subject (i.e. user mobile) requests a credential to the Idemix Issuer. For this purpose, it presents its vID to be identified against the issuer and the session ID.
- The issuer starts the Idemix proving protocol by computing a random value called nonce that is sent to the subject to ensure freshness in the transaction.
- Then, the subject computes a cryptographic token according to the credential structure (generated by the Issuer). The subject sends the issuance message and the token to the Issuer that signs the attributes with his secret key generates a proof of correctness.
- The issuer sends to the subject a cryptographic message containing both, the attributes signature as well as the proof of correctness. The subject verifies the material and stores cryptographically protected the credential in the user's wallet.

Once the subject has the Idemix credential, it can use such a credential to derive partial identities for a privacy-preserving authentication mechanism when accessing to Services, as explained in section 3.6.

3.3.3. Identity derivation

Aries identity derivation is a sequence of steps that starts with ID Proofing and ends with Mobile ID credentials issuance. Each step collects a piece of information, processes it and informs the process orchestration component of the result. If the information is needed in a successive step then it must be shared via user's App. There is no other way how the components may communicate with each other to provide protection against information leaks. The information is shared in form of a self standing token with information of which component processed and is protected by digital signature. This implies there is a trust established among components consuming each other's data. Each component may generate information needed for the feature it implements (e.g. signed biometric data needed for biometric authentication), but the Aries IdM design defines there should be no data persisted on the server side. Result of the process is a set of identity pieces: a single cryptographic credential with attributes needed vID verification and one or more biometric authenticators created during selected steps. Each of the pieces is identified by anonymous identifier and together they are linked on the server side. The link is the only part that is persisted on server and because it is only a set of random identifiers it should not be considered a privacy threat.

3.4. vID Verfication and Authentication

Each step consists of initial backend session opening with required anonymous identity reference, communication between vendor server and SDK module using vendor specific protocol and is finalized by backend call to obtain information about the result. Additional component was introduced for offline verification: a Biometric authentication appliance capable of Aries verification and live capture with one to one comparison to verify biometric data received from the App. The offline authentication flow Figure 8 considers only the Biometric appliance is online, but there would be a local network connection with the verification appliance. The App provides self-sufficient information through QR code and the appliance performs two verifications: Aries authentication and biometric comparison.

Virtual ID verification is the first step of Aries online authentication flow, Figure 5 when it is executed by Identity Verifier application. This application acts as an Identity provider application providing OpenID Connect interface. The application works as an orchestrator and uses backend services for both virtual ID verification and biometric authentication. The segregation of duties was the same as in case of the issuance process: the IdP was responsible for front-end communication, session management and audit logging, the back-end services performed their parts of the verification without knowledge of the context.

In case of face to face verification according to Aircraft boarding use case flow 8, this step is also recommended even though it is not mandatory, it provides additional security, prevents transfer of the biometric template from one device to another.

Face to face verification identified additional requirements to provide a cryptographically processed biometric template bound to Aries virtual id for machine comparison with live captured image for automated boarding process and to provide a photo for airport staff to be able to perform face to face comparison for duty-free shopping case.

3.5. Biometric Authentication

During eCommerce use case, biometric authentication may be required by the identity provider (IdP) as an alternative second factor to PIN and regardless on which biometric factor was selected it was performed as a second step after ARIES vID verification. In pilot implementation the identity provider had an option to choose facial or voice authentication by a specific parameter in authentication request.

3.5.1. Face Authentication

In order to perform face verification, the identity provider passes the live face acquisition and the encrypted template of the reference portrait to the service and ask to authenticate them. This is achieved by the integration of a biometric server taking care of coding the live acquisition and comparing the reference and live templates and accepting the authentication according to a predefined threshold. Figure 5 shows this process, where the vendor biometric verification service, in step 13, is in charge of decrypting (with his private key) the biometric token (originally generated by him during user's enrolment) presented in that moment by the user, thereby obtain from the token the reference biometric template and compare it with the live 3D motion acquisition of the face get from the user's smartphone camera.

In order to fight against spoofing and impersonation attacks, e.g. presenting fake biometric characteristics such as the usage of a photograph instead of a genuine face, the face recognition performs its work in three-dimensions based on motion captured by the smartphone camera. The techniques applied are different from the traditional ones that usually employ LBP (Local Binary Pattern) or the Fourier spectrum. Thus, different Biometric Antispoofing Methods [21] [20] such as the analysis of optical flows, movement magnification, the usage of invariants 3D Objects, or the estimation of 3D shape by the movement, are combined to perform a reliable face recognition. A patented counter-spoofing algorithm from Idemia has been implemented to detect this kind of spoofings attacks. This novel method allows applying the face recognition and biometric authentication under different conditions in terms of lighting and physical cameras employed, with the highest accuracy, realiability and performance.

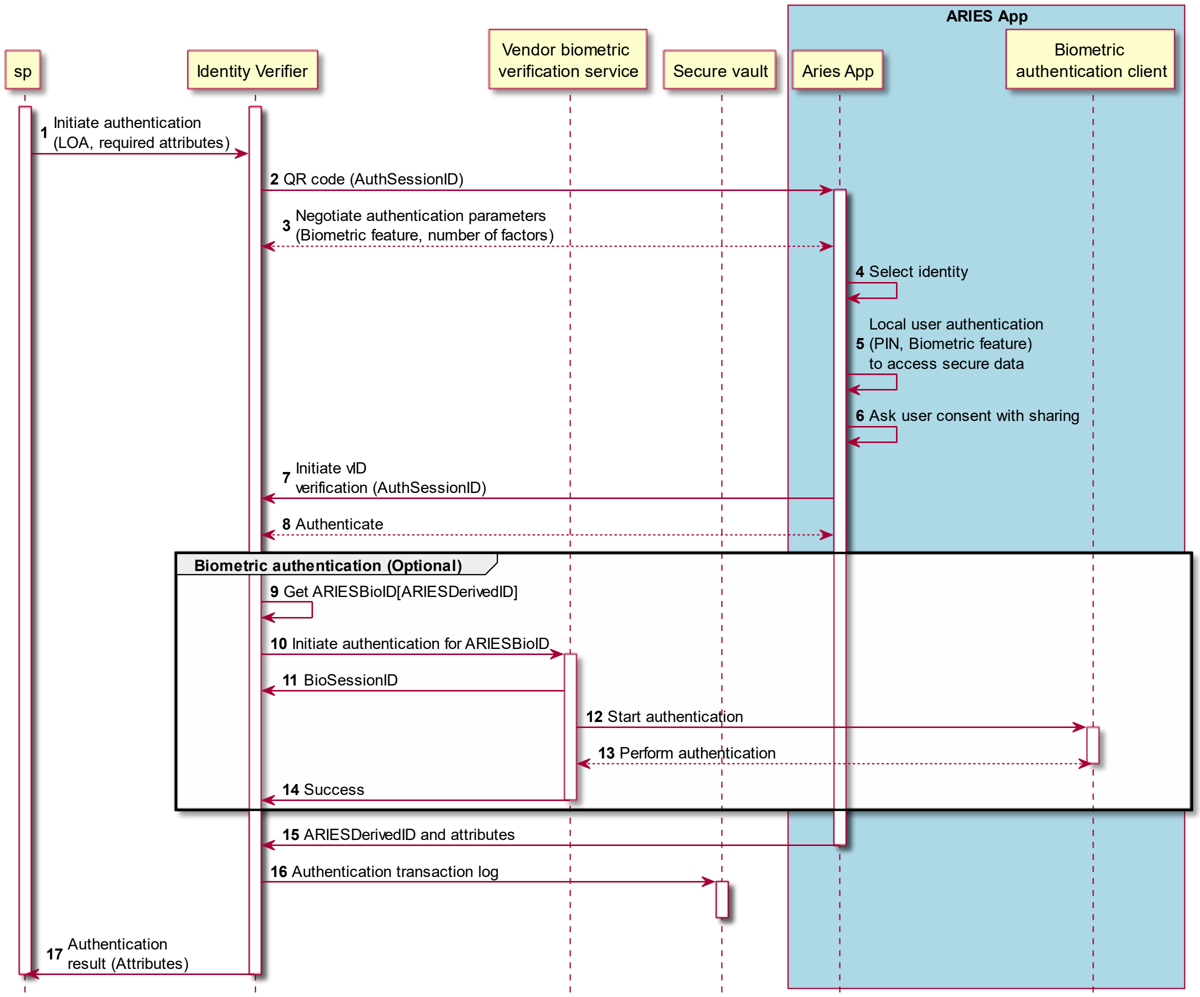

ARIES App
sp
Identity Verifier
Vendor biometric verification service
Secure vault
Aries App
Biometric authentication client
1 Initiate authentication (LOA, required attributes)
2 QR code (AuthSessionID)
3 Negotiate authentication parameters (Biometric feature, number of factors)
4 Select identity
5 Local user authentication (PIN, Biometric feature) to access secure data
6 Ask user consent with sharing
7 Initiate vID verification (AuthSessionID)
8 Authenticate
Biometric authentication (Optional)
9 Get ARIESBioID[ARIESDerivedID]
10 Initiate authentication for ARIESBioID
11 BioSessionID
12 Start authentication
13 Perform authentication
14 Success
15 ARIESDerivedID and attributes
16 Authentication transaction log
17 Authentication result (Attributes)

Figure 5: Aries online authentication flow

3.5.2. Voice Authentication

Voice authentication is performed in the same way as the enrolment: three samples of English spoken numbers were provided and verified on server side, the user is prompted to recapture if the quality was not up to expectation or verification failed.

As mentioned in Voice Enrollment chapter, the voice biometric information was stored on server side, but it was in line with the goal of the voice prototype implementation to verify existing service may be integrated into ARIES solution without excessive workload.

3.6. Foundations of Anonymous Credential Systems

In the Idemix [7] Anonymous Credential System, every Zero Knowledge Proof (ZKP) relies on the Schnorr's protocol. As described by Camenisch and Stadler in [27], the ZKP discrete logarithm is expressed as $PK\{(\alpha) : y = g^{\alpha}\}$, given a known group $G = \langle g \rangle$ of prime order q and public value $y \in G$. It means the prover knows a secret α that satisfies that g^{α} is y, so that α is equal to the discrete logarithm of y, $log_g y = \alpha$.

The prover firstly chooses a value r randomly, computes the *commitment* $t := g^r$ and sends t to the verifier. Aftwerwards, the verifier chooses another random exponent, the *challenge* c, and sends it to the prover. Next, the prover computes the *response* $s := r - c\alpha \bmod q$ and sends it to the verifier. Finally, the verifier checks whether or not

$t ?= g^s y^c$ holds. The verifier never receives the secret value α, and the verifier will not be able to compute it given t and s. Then, $g^s y^c = g^{r-c\alpha} g^{\alpha c} = g^r = t$.

Thus, in Idemix, the prover computes the *commitment* t, next the *challenge* c (computed with $\mathcal{H}$), and finally, the *response* s. A prover can compute parallel ZKPs as long as multiple t-values of each individual proof are computed. The prover also computes the same challenge c for each single proofs and integrates them in a hash. Finally, the prover generates the s-values in parallel.

In the Idemix Proving scheme the prover and verifier share a context information, the verifier generates the nonce, and the prover, non-interactively, computes the proof. The common values are equivalent to Schnorr's t, which was shared between prover and verifier. The verifier can recover some $\hat{\texttt{t}}$-values from common, c and the s-values. This is equivalent to recovering Schnorr's t from $g^s y^c$. The verifier then checks whether or not c equals $\mathcal{H}(...|\texttt{common}|\hat{\texttt{t}}|n)$ to verify if the $\hat{\texttt{t}}$-values are actually the t-values, making the proof valid. Thus, during the Idemix proof, the user with his mobile computes the t-values, the challenge c and the s-values that is sent to the verifier service to validate it.

3.6.1. ACS authentication and selective privacy-preserving showing of attributes in Aries

The main privacy-preserving authentication process and attribute proving based on Idemix, between the Prover (Aries user) and the Verifier (Service Provider) is shown in Figure 6. In Aries, when the user wishes to authenticate against a e Service provider, e.g. a duty free shop terminal, through an anonymous credentials system, he first, starts the Idemix proving process, generating ZKP explained in previous section. For this, the verifier generates a fresh QR code encoding the session URL. Next, the subject (user mobile) reads the QR code with his Aries app.

The Aries app takes the URL encoded in the QR and pass it to the wallet in order to create a new proof with the session URL. Once the proof is done, the wallet asks directly to the verifier for the presentation policy to fulfill. The verifier answers to the wallet with the presentation policy and the wallet will ask to the user to obtain confirmation (or not) about the information that is required. When the user confirms, the wallet generates a proof that fulfills the required information from the verifier and sends this proof to it. Finally, the verifier verifies the proof and tells the verdict of the whole process to the shop terminal or the merchant.

An anonymous credential can be thought of as a digital signature by the Issuer on a list of attribute-value pairs. The straightforward way for the user to convince a verifier about his list of attributes would be simply transmit it to the verifier however, this approach implies revealing all attributes, and the verifier can reuse the credential to impersonate the User. Instead, in an anonymous credential system, the User can even convince the verifier that some complex predicate over the attributes holds using ZKPs. In particular: Sum of attributes and/or constants, Product of constants, Comparatives between constants or attributes, Logical predicates are supported.

For instance in the e-commerce use case, the user have to demonstrate that his $birthdate \leq today - 18years$. In that sense, the protocol does not leak any information other than the truth of the statement meanwhile, the rest of the attributes remains private from the verifier, but so do his exact date of birth.

3.7. Identity Fraud investigation and Secure Vault

The Secure Vault is a distributed service that maintains encrypted evidences and ID correlations, facts and logs, collected during the whole identity life-cycle (ID proofing phase, bio enrollment, vID usage). It offers API to Create, Read, Update, and Delete the data stored per user. It also supports managing delegation and access control for enabling Law Enforcement Agency access in case of cyber-crime. Law Enforcement Authorities (LEAs) might be given grants to inspect and access the transaction logs stored in the Secure Vault, provided the grounds for inspection are fulfilled, e.g. an identity-related cyber-crime is perpetrated. In such as case, LEAS are given right to de-anonymizate user's identity and associated audit log data kept securely protected in the Secure Vault. Namely, LEAs, should satisfy a policy stating with particular information can be obtained along with the circumstances needed for inspection.

When an action is performed on one of the ARIES component, a event is registered in the secure vault through syslog over TLS, payload being a JSON format defined by each platform component with the valuable information. Each event is registered into a logical vault that isolates messages related to identifier of the person for this component (reminder: in ARIES, there is no global unique identifier, identifier are localized to a component).

On the deployment areas, if the legal framework enforces logs segregation or storage of a local copy the events, the functional vault component is instantiated into several physical instances and the main node will process rules according to different criteria (user country, service provider country ...) to route the messages to the vault(s). The

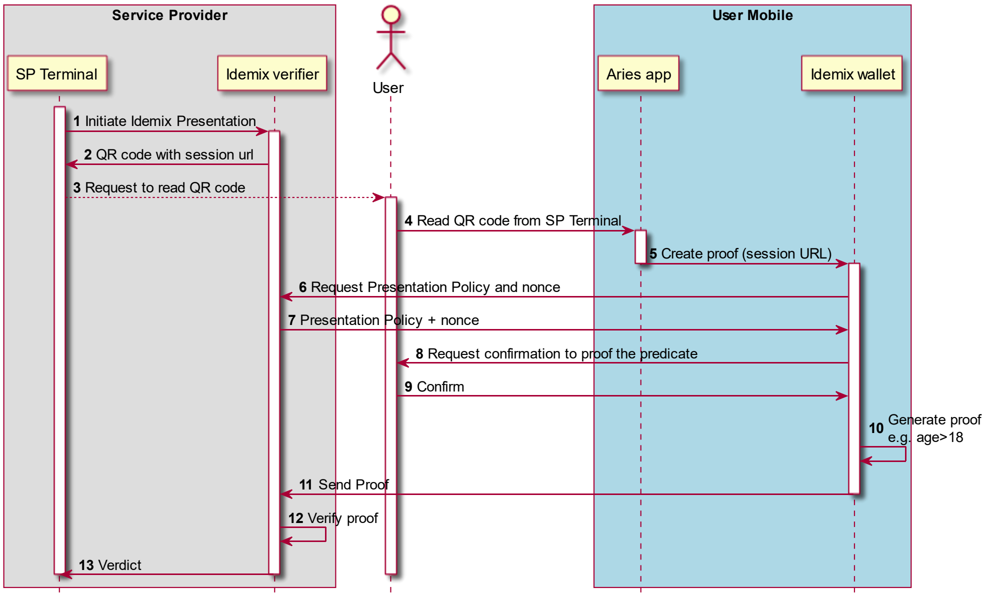

Service Provider
SP Terminal
Idemix verifier
User
User Mobile
Aries app
Idemix wallet
1 Initiate Idemix Presentation
2 QR code with session url
3 Request to read QR code
4 Read QR code from SP Terminal
5 Create proof (session URL)
6 Request Presentation Policy and nonce
7 Presentation Policy + nonce
8 Request confirmation to proof the predicate
9 Confirm
10 Generate proof
e.g. age>18
11 Send Proof
12 Verify proof
13 Verdict

Figure 6: Athentication and selective attribute disclose with ARIES based on Idemix

Secure Vault is an encrypted container that uses different keys, among them, it has a escrow key that is used when a legal request is presented. In some cases, the user figures out that someone unauthorized had access to his vault. In that case Aries vault allows access in case of suspected Identity theft. The user requests a QRCode (as a bearer token) in ARIES mobile app that will be scanned by the agent to get access to the audit trail. In addition, when an official request from a judge is received to permit vault inspection by law enforcement agencies, access someone's Secure Vault without their consent being necessary, the key previously escrow-ed is used. First, it is restored and then used to decipher the content of the corresponding vault.

4. Aries Implementation in Pilots

4.1. e-Commerce Scenario

The eCommerce scenario is based on one of the most frequent cases of virtual ID usage: a client will be logged into an internet service provider, in our case a digital shop, to buy any product using the eID and being required to share personal information. As the transaction will be online with no human intervention the process is very vulnerable to identity theft. Figure 7 represents the flow of the eCommerce login.

To perform this scenario, some important steps have to be conducted: user and eCommerce enrolment in the system, creating a vID, and following with mutual verification of these vID; agreement on attributes to be presented; biometric authentication from client; selection of specific user's attributes to be shared with site and login process on eCommerce. Three actors are involved in this use case: user (client), eCommerce website hosted by continente.pt and provided by SONAE and the identity provider, where ARIES platform plays this role validating the eID used.

In the execution of this scenario, two consecutive phases are defined. First, the vID creation process, that will allow users to generate a (or sets of) virtual mobile identity securely derived from physical official documents. In addition, ARIES IdP gives users the opportunity to link more attributes (self-claimed) to the vID than those extracted from the breeder document and store them in the ARIES token, such as delivery address or email. Second phase, where it is performed the verification of user's credentials and linkage of this client identity with existing account in the eCommerce database. In this authentication process, ARIES uses a QR code as communication mean between mobile app and website to avoid any username submission. The user must select an identity from the mobile wallet, read the QR code on the website page using the mobile device and select on the app screen any extra attribute required to be shared for the login.

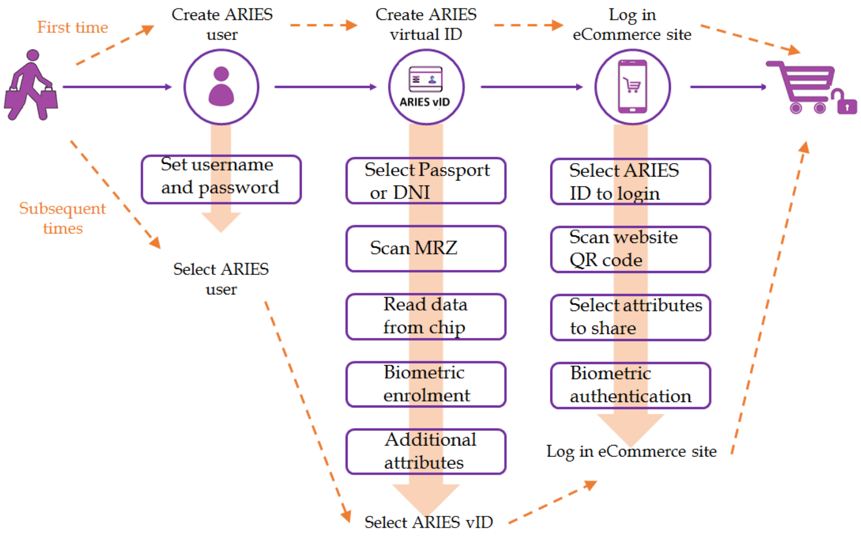


Figure 7: Login to eCommerce

4.2. *Airport Scenario*

The airport scenario is split in two main use cases. On the one hand, in the Aircraft boarding use case, the users need to demonstrate its identity in a face-to-face scenario, where High level of assurance (LoA) is demanded, i.e. live authentication with biometrics is required. On the other hand, the duty-free use case aims to validate the Aries benefits to employ Zero-knowledge proofs in face-to-face scenario, and using mobiles, to prove, in a privacy-preserving way, certain predicates about user's attributes.Both use cases are defined in the following subsections.

4.2.1. *Aircraft boarding use case*

The use case of boarding demonstrates the use of ARIES vID in the context of a physical access control, where the virtual identity which be controlled against a fresh acquisition to demonstrate strong identification: The user in front of the boarding gate is the one for whom the passport has been issued.

The first step is vID verification (Figure 8, steps 1 to 7) and has same scope as verification for web use cases. Attributes shared contain only basic information needed to verify the person is the owner of the boarding pass and processed biometric data needed for the live verification. The Biometric verifier performs the same vID verification (Figure 8, steps 8 to 15). Using the boarding pass, an ARIES derived ID and a biometric template, the boarding terminal must validate all the data to demonstrate the identity of the user. In that sense, a biometric live scan is done and verified against the Biometric verification service. Once the live verification is done, the user is fully identified.

4.2.2. *Privacy-preserving shopping in the Airport*

In this use case, a user wants to buy some kind of restricted good i.e alcohol, inside a store at the airport and wants this process to respect their privacy (Figure 6). By using the ARIES ecosystem, the user can make the purchase in a simple way. First, the user authenticates through ARIES inside the store presenting his boarding pass with the QR code.

Then, the shop assistant can verify in a privacy-preserving way, thanks to ARIES, that the passenger who wants to make the purchase complies with the requirement. i.e. if he is over 18 years old to buy some goods in the shop like alcohol beverages.

ARIES complies with the minimum disclosure principle so neither the store, nor the seller need and will not to collect extra information which means, the shop cannot get any user personal info beyond the minimal required information. Only the assurance that the user holds a valid boarding pass and the passenger's age whiting a range i.e. >18. Moreover, physical breeder documents are not needed anymore to demonstrate the age.

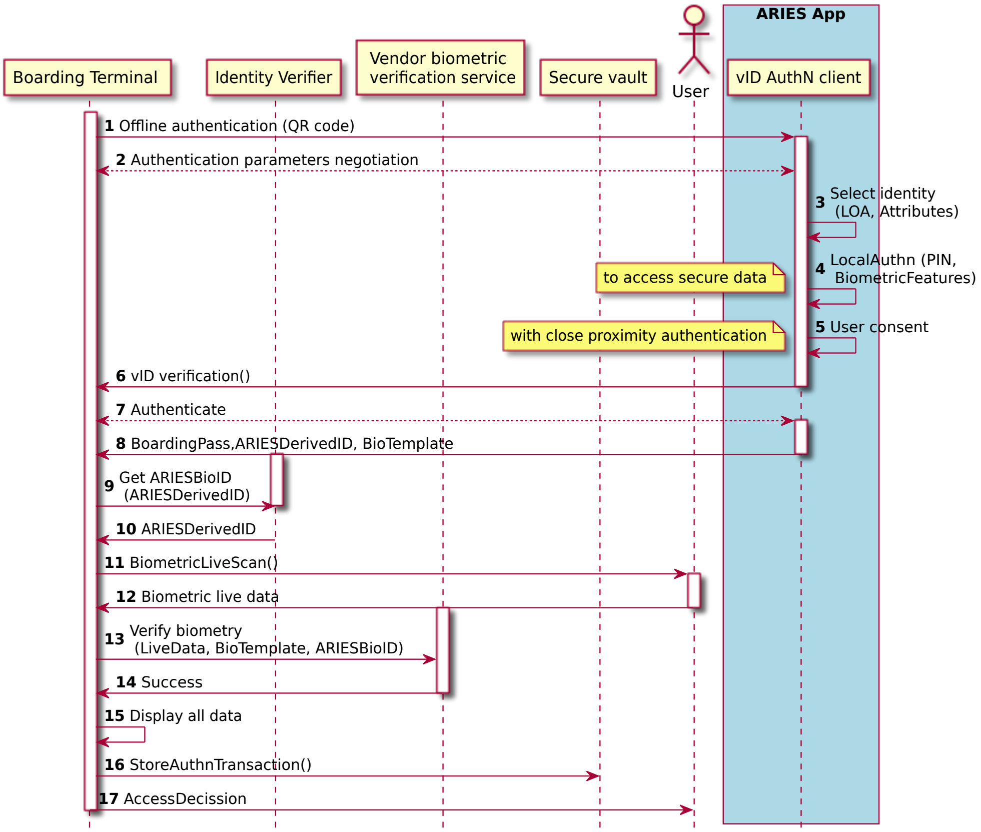

ARIES App
Boarding Terminal
Identity Verifier
Vendor biometric verification service
Secure vault
User
vID AuthN client
1 Offline authentication (QR code)
2 Authentication parameters negotiation
3 Select identity (LOA, Attributes)
4 LocalAuthn (PIN, BiometricFeatures)
to access secure data
5 User consent
with close proximity authentication
6 vID verification()
7 Authenticate
8 BoardingPass,ARIESDerivedID, BioTemplate
9 Get ARIESBioID (ARIESDerivedID)
10 ARIESDerivedID
11 BiometricLiveScan()
12 Biometric live data
13 Verify biometry (LiveData, BioTemplate, ARIESBioID)
14 Success
15 Display all data
16 StoreAuthnTransaction()
17 AccessDecission

Figure 8: Aircraft boarding use case flow

5. Security Analysis

The eCommerce scenario resembles typical use cases deployed by many organizations: remote authentication through web interface. State of the art authentication systems are usually based on symmetric (OTP, OCRA) or asymmetric cryptography (PKI, Fido). Biometric is in most cases an authentication to the token (biometric feature is used instead of PIN) or completely independent factor to the basic authentication. ID Proofing is usually done as an additional process performed after the basic using enrolment and credential issuance with only a limited link to them. The security model of the Aries solution considers following assets. 1) vID credentials, 2) ID Proofing information (information from electronic document, 2) Biometric credentials (data from biometric enrolment and personal biometric features), 3) Link that preserves relation of the aforementioned.

The solution uses standard deployment model with web browser and with similar solutions it shares same threats such as web session theft, man in the middle and man in the browser. Aries is not intended to address these threats as they have not been selected as the most frequently encountered ones. Aries vID credentials consider usage of state of the art technologies, PKI used during the pilot may be considered as one of the strongest credential technology. There is no evidence any PKI credentials have been forged based on public information if current security recommendation regarding algorithm and key strength were followed [28]. There are known weaknesses related to cryptographic devices (such as smartcards) and algorithm implementations such as predictable keys due to low entropy random numbers [29] or timing attack weaknesses due to insecure calculation implementation [30]. These weaknesses are common to all similar systems and are of the scope of Aries.

The solution considers that all private information is stored in the mobile handset, namely in a component called Mobile Wallet: a secure storage encrypting and protecting the data with selected measure (PIN, pattern, fingerprint or any other biometric feature). The IdM defines the required interface for the Wallet and considers each vendor to provide their own implementation, so as such the final security cannot be evaluated in general. The implementation provided for demonstration relied on a database storage with data protected by PBKDF2 (Password-Based Key Derivation Function) [31] with password and device fingerprint as an input.

Even though the overall concept provides privacy-by-design for persisted data, at some point the private information must be processed by the server components and at this time the real privacy depends on segregation of the components and trust level of implementations. This implies that the highest level of privacy may be achieved only if each component is operated by a separate organization and there is an process set up to ensure the implementation does not store data that are supposed to be transient. Both of these may be done by regular organizational audits.

5.1. Issuance process security analysis

Issuance process consists of several steps when all the assets are created and linked together. The process must take place on a single device and, if finished, the new vID will be stored on the device as shown in the the Aries App screen (Figure 9). The communication considers TLS usage with server authentication and optional certificate pinning. Following threats have been identified:

- Attacker gets hold of the exchanged data.
- Attacker steals the session and performs issuance of the credential into his device, but with user's ID Proofing and biometric data.
- Attacker tries to issue credential on fake document.
- Attacker tries to issue credential using stolen document.

The data exchanged between the App and server are protected on several levels. The communication between the App and all the servers uses TLS and it is recommended that all the SDK parts use certificate pinning to their respective server counterparts. The protocol defined considers exchange of JSON web tokens with encryption of sensitive data and the encryption was implemented in the pilot. The session and link between the ID Proofing and vID issuance is protected by the fact that data read and used during the enrolment are stored in the App and subsequently used for issuance. In case of the attack the attacker would need to steal also information from Mobile Wallet. This can be considered as a significant protection of the session.

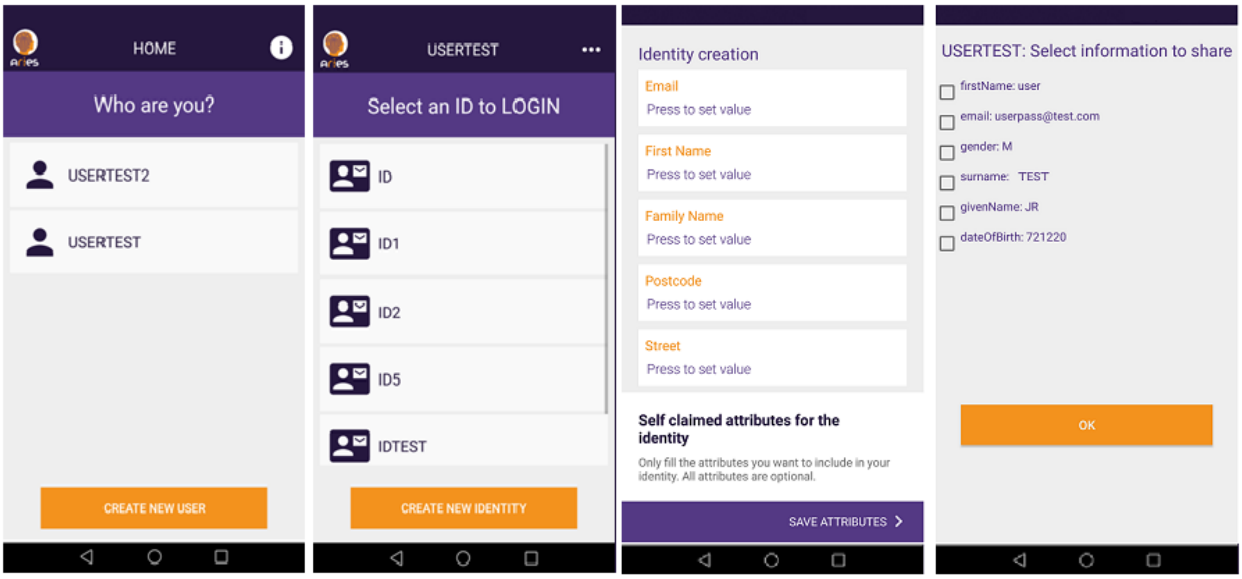
Document verification done during the Aries ID Proofing step covers ICAO passive and active authentication, resistance to document forgery is the same as border control process deployed by most of the states. The process may be improved by additional biometric verification using protected information from electronic document (such as fingerprint or iris verification), but we considered that as non-governmental organization the Aries issuer would not request certificates for terminal authentication needed to access the information. Issuance of credentials based on stolen documents considers usage of genuine document with a subsequent attack on the biometric verification ,either by lookalike person or with a prop of quality ranging from simple printed photo to 3D printed mask. Different kinds of countermeasure are used in order to fight against frauders like :

- 3D face reconstruction: used to avoid paper / flat screen attacks.
- Image spectrum analysis to detect if it is an image displayed on a screen.
- Visual challenge response : basic mask will be identified and rejected.

There is a trade-off between FAR/FRR, and enforcing a too strict set of rules (reducing FAR) will make FRR much higher. And high quality latex mask will not be detected without specialized hardware.

5.2. Authentication process security analysis

Authentication process follows the similar pattern as the issuance: there is a single orchestrator that controls the whole process and several services implementing the authentication steps (Aries vID verification, face verification, voice verification and others). The process considers following protected assets: 1) Authentication session; 2) User personal information (attributes); 3) Biometrics.



Email
Press to set value

First Name
Press to set value

Family Name
Press to set value

Postcode
Press to set value

Street
Press to set value

Self claimed attributes for the identity

Only fill the attributes you want to include in your identity. All attributes are optional.

□ firstName: user
□ email: userpass@test.com
□ gender: M
□ surname: TEST
□ givenName: JR
□ dateOfBirth: 721220

Figure 9: Users vID list ARIES screens (left) and Self-claimed attributes app screens (right)

The process must ensure the session is finished as whole, and all the steps are performed using the same identity. The attacker may, for example, try to perform vID authentication with stolen vID and then biometric authentication with his vID. This is ensured by the split of the authentication between front-end and backend-calls where the attacker may be able to intercept and tamper with the data exchanged through the front-end, but the back-end calls will ensure the session inconsistency is detected.

User personal information may be threatened by two situations: the data are disclosed to the attacker during the authentication process or the vId discloses more that the user consented to share. The first threat is mitigated by the common strategy by the solution: mandatory TLS usage with optional certificate pinning with additional application level encryption, second threat relies on Mobile Wallet implementation: it must make sure no data leave Mobile Wallet without user consent. Aries considers each function call to obtain data has exact authorization procedure associated and the authorization is applied to whole identity and each item separately: user enables access to his identity, but to access the personal information additional step is needed. The verification process differs for each vID technology. During verification process of basic PKI credentials personal information is exchanged after vID verification as attributes linked to the vID, during Idemix verification the data are exchanged. From this point of view the Idemix approach, it is more privacy-friendly and provides much better solution. The PKI still has a few issues: public key and identifier used in certificate are unique and may be used to track the user's activity among Service Providers. Nonetheless, this issue may be removed by deployment: additional proxy may be deployed in front of the IdP and manage the communication with the Service providers. The proxy would work as a relying party for the backend IdP and attributes provided by the IdP would be encrypted by Service Provider key in order to protect them from disclosure to the proxy.

The biometric authentication may consider two approaches: lower level of security when the authentication is only local: specific credentials are issued during the enrolment and the biomertic feature is used to either unlock the credentials or to provide input for crypto operation. This has an advantage the biometric information does not leave the mobile device during authentication and thus cannot be disclosed. On the other hand, this means the attacker holding the device (when stolen or via malware) may be able to bypass the biometric authentication. Biometric authentication using server side verification provides more reliable authentication but has the weakness of data disclosure during the communication. For the latter case Aries enforces privacy rule that the verification must be based on transient data and all data must be erased after the verification in order not to retain any user information on server side.

6. Performance evaluation

This section describes the evaluation carried out to demonstrate the feasibility and performance viability of the Aries IdM in the two instantiated Pilots defined above.

6.1. eCommerce Evaluation

6.1.1. eCommerce Technical feasibility

The implementation of the eCommerce scenario uses existing functional services that are bound together with the orchestrator services for both issuance and authentication. The proposed architecture follows the state of the arts approach and implementation using REST API is simple. There were only a few modifications needed on the existing services to be compliant with the security and privacy requirements (such as logging into the Secure Vault), rest of the development may be considered as a lightweight proxies working as a boiler plates.

Good proof the architecture is suitable for such use case was provided during integration with voice authentication service originally dedicated to a different use case: server side voice verification. Integration with the service consisted of development of a thin proxy managing session and state of the process, and integration time was very short. This suggests the Aries architecture is flexible enough to be able to integrate new services originally not targeted for user authentication that may come in future.

6.1.2. eCommerce Testbed description

The creation of the ARIES vID is only needed for the first time. Subsequent times the user wants to log in to the eCommerce it is not needed to create the vID again but select the vID to be used for the login. The target response time for all actions is 2 seconds. In server side measurements it is considered pure reaction time without user interaction and measure duration for each step using reference hardware (8 CPU cores, 8 GB RAM). Issuance process orchestration is simple and according to measurements it is far from being the bottleneck of the solution.

Issuance of vID PKI credential issuance is time consuming due to signature process (X509 and Attribute certificates). The testbed reaches around 100 transactions per second before reaction time rose above the 2 seconds. PKI authentication process is inline with expectations of the PKI based services. In the testbed we were able to reach around 80 transactions per second before the reaction time rose.

In server side, the Aries APIs for secure vault, ID proofing, biometric enrolment and authentication and server middleware components, the hosting has been done on a virtualized environment with 4 cores and 8 GB. Additional security components (firewall, reverse proxy) have been added to enhance security in another virtual machine in front of the components. The response time for the various unique operations once the data have been uploaded to the server - excluding the network transit time - is in 97% less than 1.2 s, 81% being less than 400ms.

6.1.3. User experience

User acceptance is one of biggest concerns. Even with perfect architecture and flawless privacy the proposal would fail if in the end users would not accept it. Since ISO defines the concept of usability as the ability of the users to achieve their goals effectively, efficiently and satisfactorily [32], the mobile application has been designed having in mind two perspectives: (i) smoothness and intuitiveness of the enrolment, as it is the key task for identity derivation process and (ii) usage and response times needed to perform all use cases, aiming to attract users to this kind of vID technologies. With these two targets, the user interface of the mobile application follows a minimalistic and clear screens, guiding the user through the different steps. All actions can be performed with reduced number of clicks on buttons, including some icons and graphics to help the user to understand the process.

During the eCommerce evaluation, the feedback from the user experience was gathered using different methods (i.e previous online survey, questions on-site and round tables during demonstrator). 29 people participated in the practical exercise during 3 days, reaching 82% of successfully biometric enrollment processes, taking 130 seconds in average to complete the whole procedure defined in section 3.2 (including ID Proofing, biometric enrollment and virtual ID issuance as a first step and biometric authentication and login into website as second step). The rest of unfruitful cases were due to physical problems with passport during chip reading. The tester's comments about usability is good, very practical and easy to use. In comparison to social logins, despite their speed, the clear majority preferred ARIES solution, as there is lack of trust in social media and ARIES has a strong and trusted way of virtual identity management. Overall positive feedback given can be compiled in the the following topics: (i) users stated that the focus on privacy, control of data and security of the solution was outstanding and they were excited that such a tool might be available in the future; (ii) regarding look and feel, users recognized ARIES app had a very good and intuitive design, including visual guidelines for different steps; (iii) the control of user's data in the ARIES wallet and vault was much important and a huge plus to adopt this kind of solution, stating that they would likely use the service as it will be available in the market.

6.1.4. Performance evaluation

In the mobile application, the user can execute all the actions with simple clicks on buttons. The Aries enrolment and the eCommerce use case processes requires several steps the first time it is completed.

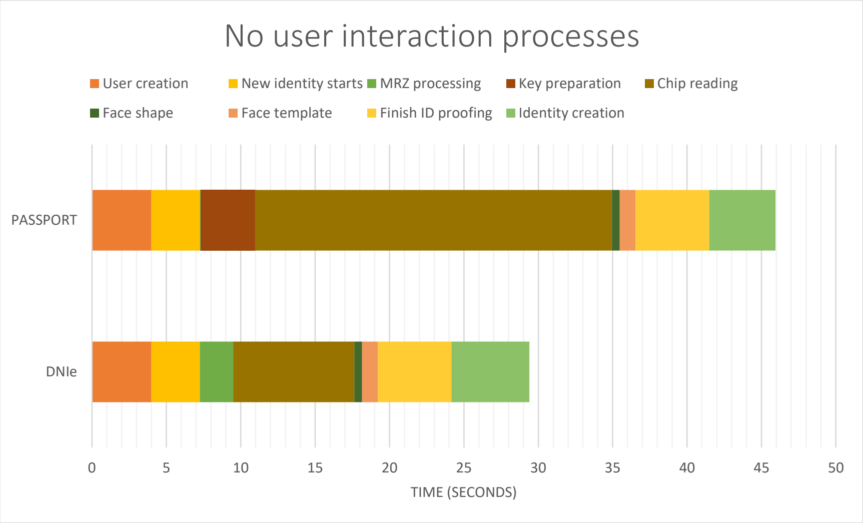


Figure 10: No user interaction processes

Figure 10 shows the performance times of the main *No user interaction processes*. The times shown are the averages of 50 executions. The performance times includes the main 4 phases. 1) Enrolment and ID-proofing (either Passport-based or eID-based), 2) Biometric enrolment, 3) vID issuance and authentication, 4) Biometric authentication. It should be noticed that phases 1) and 2) are identical in both scenarios eCommerce and Airport Scenario.

6.1.4.1 Enrolment and ID-proofing performance

The user profile creation (with user and password) takes less than 4ms on average. The user previously created can add a new identity under this profile. To that aim, the mobile first contacts the Issuer server to prepare the webservice for identity creation. This process lasts 3,24 seconds. It should be noticed that all times includes network transit times, to show the real user experience usability.

Passport-based enrolment performance: the performance includes the MRZ reading by the smartphone after the users gets the OCR of the MRZ. Once the MRZ is scanned, the app takes 72ms (average) to process the MRZ information and an average of 3,638s to prepare the key for reading the chip. The server is contacted to validate the passport chip, by using Basic Access Control (BAC) and Active Authentication [25]. To this aim, the user is required to approach the passport chip the back of the phone, where NFC is placed. Once the chip is detected, the app starts to read the chip, taking an average of 24.001s to complete the action. Figure 11 recaps the main performance times related to eID documents processing.

Spanish eID enrolment performance: the camera will be activated to read the MRZ of the spanish official eID (called DNIe). The app takes 2,247s (average) to process the MRZ information. The app requires the user to put the DNIe chip on the back of the phone, where NFC antenna is placed. Once the chip is detected, the app starts to read the chip, taking an average of 8,138s to complete the process and validate the chip data.

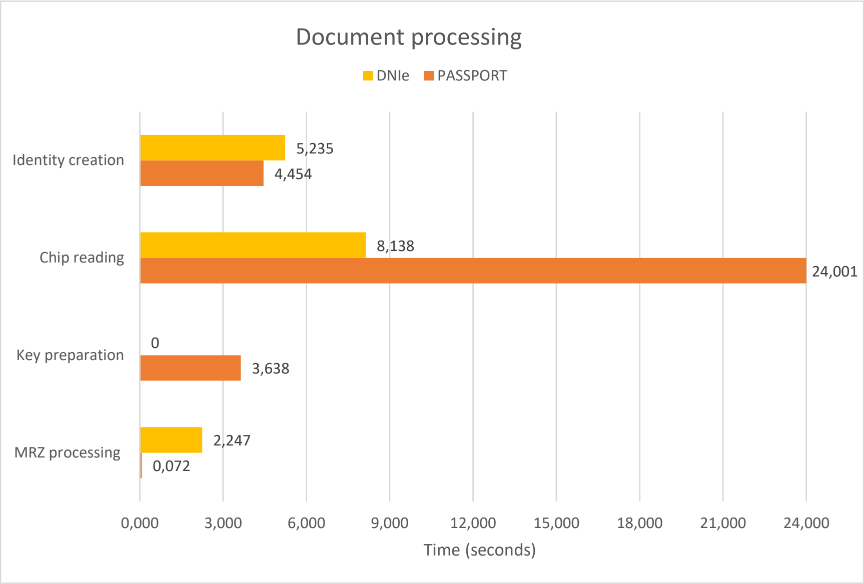


Figure 11: Document processing comparison

6.1.4.2 Biometric enrolment performance

Biometric enrolment takes on average 523ms to prepare the screen in the mobile with face shape. The user must center the head on this shape and turn the face to the left meanwhile the app is recording the action to prove liveness. Once the face acquisition is done, depending on the user interaction, the app will generate the face biometric template, taking an average of 1.072s, and then communicate with the biometric server to obtain the biometric token in the devices, taking 4.939s. Then the user is prompted to add any self-claimed attribute to the identity, Figure 9, such as email, address, or nickname entering the data in the corresponding field. The process identity creation lasts 4.454ms to complete the task. It should be noticed that the memory used in the mobile during a complete process of vID creation with biometric enrollment, the app used an average of 297MB of RAM.

In the server side, the biometric enrolment and authentication require almost the same time (150ms) (coding image to template being respectively much longer than matching two templates). The IPV requests are a little bit longer as different components are used with point to point security connections requiring TLS connections with client and server certificate authentication.

6.1.4.3 vID issuance and authentication performance

Once the identity/ies is/are created, the user can select one to be used during the login in the eCommerce scenario. The web page of the eCommerce will display a QR code in the screen to be scanned by the ARIES app. The user should short press in the wanted identity and the app will activate the camera of the device to read the QR. When the QR is scanned, the app takes an average of 287ms to process the QR. After reading the QR, the app will display to the user the different attributes included in the identity selected previously. The user should click on each attribute she/he wants to share with the service provider of the eCommerce.

6.1.4.4 Biometric authentication performance

Biometric authentication is required to finish the login process in the eCommerce portal through Aries. This process requires first face recognition, by creating the face shape to be displayed to the user in 881ms proving the live check centering the head and turning the face to the left (929ms). The biometric verification in the server side takes on average 3,51s to send the biometrics to the server and verify them. Namely, the time taken to send the biometric token signed by the server (and stored in the mobile), together with the fresh face capture with motion, decrypt the biometric token to obtain the template, validate signatures and compare both biometric templates.

6.2. Airport Evaluation

6.2.1. Evaluation of the authentication process with boarding terminal

During the airport evaluation different performance measurements have been gathered:

- *Registration success rate*: First, it was identified that UK new passports were not eligible due to error in MRZ scanning. Then, users were failing at least once during passport contact-less chip reading as the NFC communication between most smartphones antenna and the document requires no movement. They were also some communication errors probably due to the use of the active challenge passport authentication. This mode was chosen to ensure that the passport is really challenged and that this is not a registered copy.
- *Enrolment time*: this time was several minutes split in about 45 seconds for the passport reading operation, 30 to 60 seconds to acquire face, demonstrate liveness and upload the resulting picture to server. Then 95% of the requests for server processing operations are below 1.2 seconds, the rest of the time being the end-user journey in the application and end-user help reading.
- *Registration false acceptance*: There was no false acceptance identified.
- *Registration false rejection*: several liveness checks failed. But once this check has been passed, no rejection has been observed during the facial matching.
- *Boarding time*: A passenger first try was typically around 20 seconds, being later tries about 10 seconds, spending mostly of the time to get the QRCode acquired by the document reader. This part is known to be optimizable by using smaller biometric template, allowing the use of less dense QRCode, faster to be read by the document reader. The face matching was done really fast (2 to 3 seconds) as soon as the person is not completely still (which adds a few seconds).
- *Boarding false acceptance*: There was no false acceptance identified.
- *Boarding false rejection*: Only the use cases where the face is partially covered (typically by hiding one eye with a hand) - or if two people have been identified by the camera - have been rejected. Meaning no false rejection was identified during this session.

6.2.2. Evaluation of Idemix PPI attribute proving

In order to evaluate the performance of the solution based on Idemix Personal Private Information (PPI) attribute proving, time measures have been taken for the following cases. 1) Idemix credential issuance, 2) Idemix attribute proof generation, 3) Idemix attribute proof verification.

The measurements take into account the a credential structure having as attributes: 1) First name, 2) Surname, 3) Birth Date, 4) Photo hash. The attributes have an average size of 10 bytes with the exception of the photo hash attribute, which has an average size of 70 bytes. In general, a credential generated in the Aries APP has an average size of 100 bytes. With this information, a real credential have been generated in the ARIES App with 94 bytes of size. Having the new credential, the next step has been to carry out the Idemix credential issuance process. As result of performing the issuance process 50 times, an average time of 2608.6 ms has been obtained. Next, the time measurement for Idemix attribute proof generation and verification has been carried out bearing in mind that the credential has four possible attributes and that the service requires in all cases, at least, that the user's age is equal or greater than 18 years in this scenario.In that sense, the minimum case that has been measured is the generation and verification of a proof for a single attribute (Date of birth) and the most complete case for all the attributes. The results obtained can be seen in the following figure 12.

From the previous results, it can be easily observed that the inclusion of the photo hash attribute significantly increases the generation and verification time however, the subsequent inclusion of attributes with smaller sizes does not represent a significant change. The times obtained in the Wallet app for generation and verification are mostly the same average values. This behaviour is also reproduced in the server where the verification token process takes part.

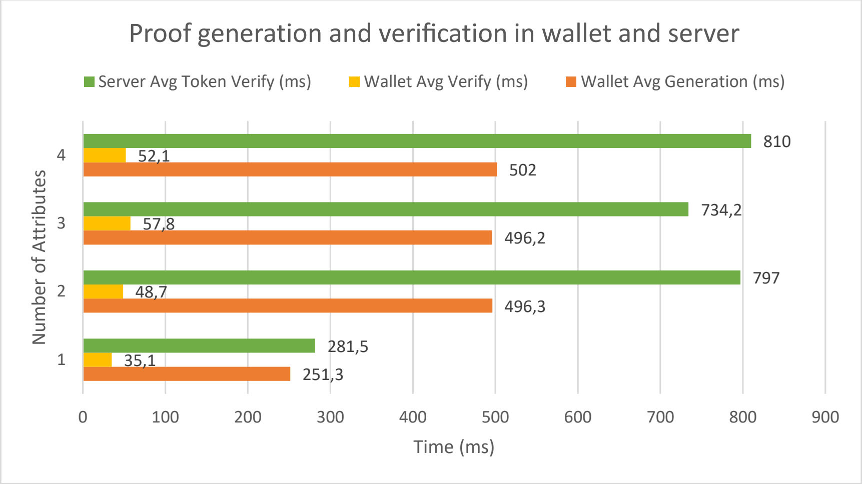


Figure 12: Proof generation and verification in wallet and server based on Idemix

7. Conclusions

ARIES IdM system aims to establish a privacy-preserving and reliable identity ecosystem that combines various security technologies, such as Anonymous Credential Systems and biometrics, with mechanisms for deriving virtual credentials from breeder documents. This paper has presented the novel Aries IdM framework that has been designed with particular emphasis on biometrics, innovative processes such as privacy-by-design, zero knowledge proofs, future extendability and implementation flexibility. Flows have been defined for all processes needed for two main use cases: web authentication and face to face verification during plane boarding or duty-free shopping, and for supporting use cases of enrolment and incident resolution.

Tests have been conducted on pilot implementation showing the usability of the ARIES IdM ecosystem and its performance for carrying out their expected task. The results proved feasibility and applicability to manage efficiently privacy-preserving, and user-friendly manner user's virtual identities in different contexts. Small scale pilots has demonstrated successfully new approach to web authentication and replacement of traditional boarding pass and passports/documents by a virtual credentials kept securely in mobile devices, while respecting his privacy and maintaining performance authentication with biometric times. Moreover, the duty-free use case has shown the Aries' benefits for user's to preserve their privacy in face-to-face and mobile authentication scenarios, revealing minimal information when Zero Knowledge Proofs were used instead of user's attributes in plaintext.

As future work, current IdMs systems with classical web interfaces, like Aries, and privacy solutions, such as Idemix, may be combined using a distributed and oblivious model approach to segregating responsibilities of IdM, thereby increasing user's anonymity against IdM that might trace users, while improving, at the same time, user's usability and backwards compatibility with current IdM standards.

Acknowledgements

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). It has been also supported by a postdoctoral INCIBE grant "Ayudas para la Excelencia de los Equipos de Investigación Avanzada en Ciberseguridad" Program, with code INCIBEI-2015-27363.

References

[1] Internet Organised Crime Threat Assessment (IOCTA), Tech. Rep. ISBN 978-92-95200-94-4, EUROPOL, European Union Agency for Law Enforcement Cooperation (2017).

[2] J. Camenisch, A. Lysyanskaya, An efficient system for non-transferable anonymous credentials with optional anonymity revocation, in: Advances in Cryptology—EUROCRYPT 2001, Springer, 2001, pp. 93–118.

[3] J. Hughes, E. Maler, Security assertion markup language (saml) v2.0, Tech. rep., Organization for the Advancement of Structured Information Standards (2005).

[4] N. S. et al., OpenID Connect Core 1.0 (2014).
URL `http://openid.net`

[5] E. D. Hardt, The oauth 2.0 authorization framework (2012).

[6] J. Torres, M. Nogueira, G. Pujolle, A survey on identity management for the future network, IEEE Communications Surveys Tutorials 15 (2) (2013) 787–802. `doi:10.1109/SURV.2012.072412.00129`.

[7] J. Camenisch, E. Van Herreweghen, Design and implementation of the idemix anonymous credential system, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS '02, ACM, New York, NY, USA, 2002, pp. 21–30.

[8] A. Tobin, D. Reed, The inevitable rise of self-sovereign identity, The Sovrin Foundation (2016).

[9] J. B. Bernabé, J. L. H. Ramos, A. F. Gómez-Skarmeta, Holistic privacy-preserving identity management system for the internet of things, Mobile Information Systems 2017 (2017) 6384186:1–6384186:20. `doi:10.1155/2017/6384186`.
URL `https://doi.org/10.1155/2017/6384186`

[10] J. L. C. Sanchez, J. B. Bernabe, A. F. Skarmeta, Integration of anonymous credential systems in iot constrained environments, IEEE Access 6 (2018) 4767–4778. `doi:10.1109/ACCESS.2017.2788464`.

[11] H. Gunasinghe, E. Bertino, Privbiomtauth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones, IEEE Transactions on Information Forensics and Security 13 (4) (2018) 1042–1057. `doi:10.1109/TIFS.2017.2777787`.

[12] E. Ben-Sasson, I. Bentov, Y. Horesh, M. Riabzev, Scalable, transparent, and post-quantum secure computational integrity., IACR Cryptology ePrint Archive 2018 (2018) 46.

[13] J. Camenisch, A. Lehmann, G. Neven, Optimal distributed password verification, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-16, 2015, 2015, pp. 182–194. `doi:10.1145/2810103.2813722`.
URL `https://doi.org/10.1145/2810103.2813722`

[14] S. Agrawal, P. Miao, P. Mohassel, P. Mukherjee, PASTA: password-based threshold authentication, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, 2018, pp. 2042–2059. `doi:10.1145/3243734.3243839`.
URL `https://doi.org/10.1145/3243734.3243839`

[15] R. T. Moreno, J. B. Bernabe, A. Skarmeta, M. Stausholm, T. K. Frederiksen, N. Martinez, N. Ponte, E. Sakkopoulos, A. Lehmann, Olympus: towards oblivious identity management for private and user-friendly services, in: 2019 Global Internet of Things Summit (GIoTS), 2019, pp. 1–6. `doi:in-press`.

[16] N. K. Ratha, J. H. Connell, R. M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM systems Journal 40 (3) (2001) 614–634.

[17] G. Lovisotto, R. Malik, I. Sluganovic, M. Roeschlin, P. Trueman, I. Martinovic, Mobile biometrics in financial services: A five factor framework, Tech. rep., Technical Report CS-RR-17-03, Oxford University (2017).

[18] J. Unar, W. C. Seng, A. Abbasi, A review of biometric technology along with trends and prospects, Pattern Recognition 47 (8) (2014) 2673 – 2688. `doi:https://doi.org/10.1016/j.patcog.2014.01.016`.
URL `http://www.sciencedirect.com/science/article/pii/S003132031400034X`

[19] E. J. Kindt, The Risks Involved upon the Use of Biometric Data and Biometric Systems, Springer Netherlands, Dordrecht, 2013, pp. 275–401. `doi:10.1007/978-94-007-7522-0_4`.

[20] R. Ramachandra, C. Busch, Presentation attack detection methods for face recognition systems: a comprehensive survey, ACM Computing Surveys (CSUR) 50 (1) (2017) 8.

[21] J. Galbally, S. Marcel, J. Fierrez, Biometric antispoofing methods: A survey in face recognition, IEEE Access 2 (2014) 1530–1552.

[22] A. Czeskis, J. Lang, Fido nfc protocol specification v1. 0, FIDO Alliance Proposed Standard (2015) 1–5.

[23] P. Chawdhry, I. Vakalis, Use of epassport for identity management in network-based citizen-life processes, in: M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, G. Zhang (Eds.), Privacy and Identity Management for Life, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 122–133.

[24] J. B. Bernabe, A. Skarmeta, N. Notario, J. Bringer, M. David, Towards a Privacy-Preserving Reliable European Identity Ecosystem, Springer International Publishing, Cham, 2017, pp. 19–33. `doi:10.1007/978-3-319-67280-9_2`.
URL `https://doi.org/10.1007/978-3-319-67280-9_2`

[25] I. Doc, 9303, machine readable travel documents, part 1–machine readable passports, 2006, International Civil Aviation Organization.

[26] J. Camenisch, et al., Specification of the identity mixer cryptographic library, Tech. rep., IBM Research - Zurich (2013).

[27] J. Camenisch, M. Stadler, Efficient group signature schemes for large groups, Advances in Cryptology—CRYPTO'97 (1997) 410–424.

[28] E. Barker, A. Roginsky, Transitioning the use of cryptographic algorithms and key lengths, Tech. rep., National Institute of Standards and Technology (2018).

[29] M. Nemec, M. Sýs, P. Svenda, D. Klinec, V. Matyas, The return of coppersmith's attack: Practical factorization of widely used rsa moduli, in: ACM Conference on Computer and Communications Security, 2017.

[30] W. Schindler, Optimized timing attacks against public key cryptosystems, Statistics Risk Modeling 20 (2002) 1–4.

[31] B. Kaliski, Rfc 2898; pkcs# 5: Password-based cryptography specification version 2.0 (2000).

[32] I. Iso, 9241-11: 2018 (en) ergonomics of human-system interaction—part 11: Usability: Definitions and concepts, International Organization for Standardization, Geneva, Switzerland (2018).