FCT-9-2015: Law Enforcement Capabilities topic 5: Identity Management

ARIES

"reliAble euRopean Identity EcoSystem"

D4.1 – ARIES Prototype Instantiation

Due date of deliverable: 31-8-2018
Actual submission date: 31-8-2018

Grant agreement number: 700085 Lead contractor: Atos Spain sae (Atos)

Start date of project: 1 September 2016 Duration: 30 months

Revision 1.0

Project co-funded by the European Commission within the EU Framework Programme for Research and Innovation	
Dissemination Level	
PU = Public, fully open, e.g. web	✓
CO = Confidential, restricted under conditions set out in Model Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC.	
Int = Internal Working Document	

D4.1 – ARIES Prototype Instantiation

Editors

Jorge Bernal Bernabe, Antonio Skarmeta Gómez (UMU)

Reviewers

Sonae, Atos

31-08-2018

Revision 1.0

The work described in this document has been conducted within the project ARIES, started in September 2016. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700085. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Document History

Version	Date	Author(s)	Description/Comments
0.1	04-04-2018	Jorge Bernal (UMU), Antonio Skarmeta	Initial ToC
0.2	05-04-2018	Jorge Bernal (UMU), Antonio Skarmeta	Contribution in section 2 – Use cases
0.3	30-07-2018	Jorge Bernal (UMU), Antonio Skarmeta	Major contribution in section 3.
0.4	21-08-2018	Jorge Bernal (UMU), Antonio Skarmeta	Updated version that include suggestions from ATOS, Gemalto.
0.5	24-08-2018	Javier Presa (Atos)	Update sections 1 and 2
0.6	27-08-2018	Tiago Oliveira (Sonae)	Additional comments on section 2 and section 3.
0.7	29-09-2018	David Martin (GTO) and Sébastien Bahloul (IDM)	Update section 3
0.8	30-08-2018	Jorge Bernal (UMU)	Final version

Executive Summary

This document describes the concrete instantiation done for the setup of the demonstrators, indicating the different components being considered and the whole integration being carried on for the deployment. Namely, this document describes the instantiation and set up of the Aries architecture and its associated components according to the functional needs and requirements defined for the prototypes demonstrators. To this aim, the document firstly defines the use cases from a functional point of view. Then, section 3 describes the set-up and instantiation of the components for the eCommerce scenario and Airport scenario.

Contents

List of Figures

1 Introduction

Aries main goal is to design and develop a reliable identity ecosystem taking into consideration and incorporating, to the extent possible, new technologies, processes and security features to ensure high quality secure credentials for secure and privacy-respecting physical and virtual identity management processes. Aries aims 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.

To achieve this goal, Work Package 4 is dealing with the instantiation of the ARIES technology into a format that allows the results to be tested and validated in two end-user driven demonstrators. The first demonstrator focuses on the ARIES innovations relating to the online (biometric) authentication and proofing, identity derivation, in the scope of an eCommerce scenario, whereas the second demonstrator focuses on strengthen the security, trust and privacy in identity-related processes in the scope of Airport scenarios, namely, boarding and duty-free shopping.

Likewise, task 4.1 aims to provide the concrete instantiation of the ARIES platform provided by task 3.4 to support the requirements and functional needs of the prototype demonstrator of task 4.3 and task 4.4. The integration activities build in the operational requirements and sets out the exercise planned in the prototype demonstrations.

Concretely, this document describes the particular set-up and instantiation of the demonstrators, defining the set-up of the architectural components being considered as well as the integration accomplished for the deployment of the prototypes.

2 Aries scenarios: functional description and added-values

This section includes an updated and summarized functional description of the use cases originally defined in the restricted deliverable D2.1.

2.1 *Aries eCommerce proposed Scenario, Actors and their responsibilities*

This scenario 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 order to address or prevent different identity theft use cases identified by law enforcement agencies, a typical eCommerce scenario has been re-designed to include ARIES technology.

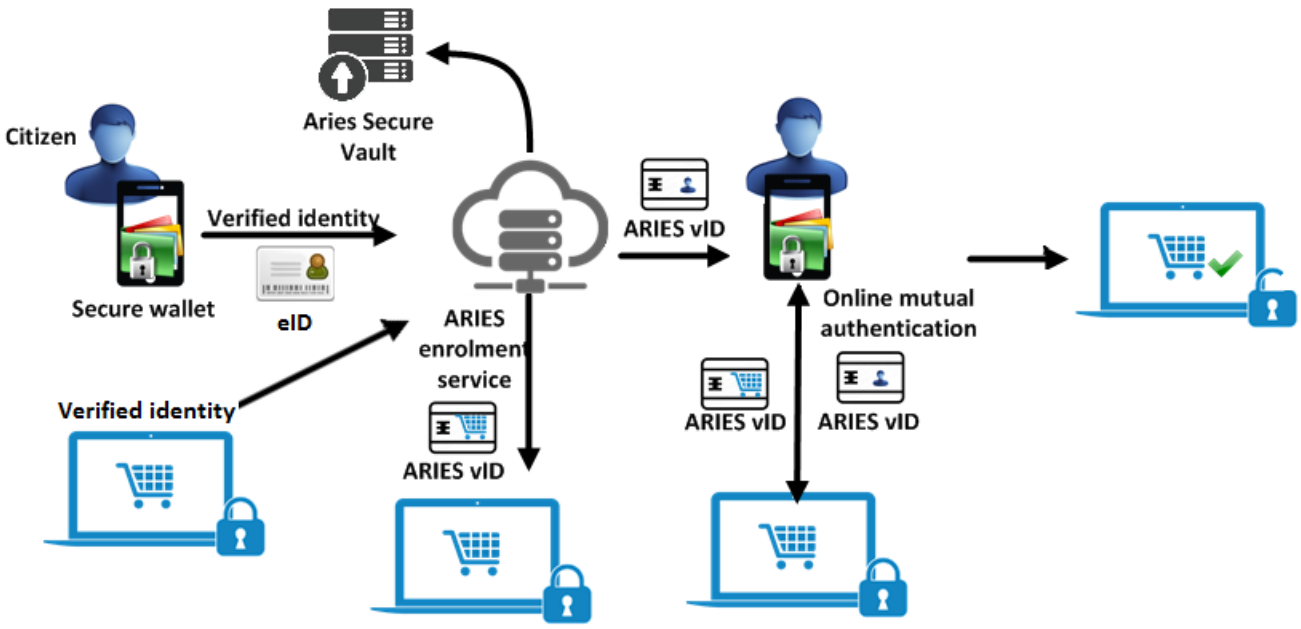

Figure 1 - eCommerce scenario

These are the steps that users and service providers must follow to use an ARIES digital identity in the eCommerce scenario:

- Both, eCommerce provider and users need an ARIES digital identity obtained through ARIES enrolment by using digital certificates and eIDs;
- The service provider will express through ARIES the minimum attributes, including required level of assurance, they require for customers' purchases. These minimum attributes required in the eCommerce instantiation are Name, Email and a password. It is possible to optionally add other attributes.
- When the users are required to be authenticated in the eCommerce site, they will select in their mobiles the digital identity of their choice that meets the provider's requirements.
- ARIES components at the eCommerce provider will check the validity of the selected mobile identity and, require a biometric authentication using the mobile camera.
- Once the users´ identity is verified, the eCommerce provider performs the authentication and the corresponding login sharing only the personal information included in the attributes.

Actors:

The User

The user is the usual eCommerce client that would like to log into the website.

For the demonstrator of the eCommerce, employees from the SONAE departments of Innovation, Ecommerce and associated partners- MO, SportZone and Zippy-, were invited to register and be authenticated into the Aries platform and then to register and log-in Chef Online.

ARIES Identity Provider

The ARIES Identity Provider is the entity that provides and validates the user ID to the eCommerce website, where the user is identified.

eCommerce Website

The eCommerce website is hosted by continente.pt, which is the beneficiary of the authentication service, and supports verified users in their processes, allowing for a smother and securer customer experience. This website is provided by SONAE and for the demonstrator it was used a testbed webpage of the Chef online, a section of the continente.pt website.

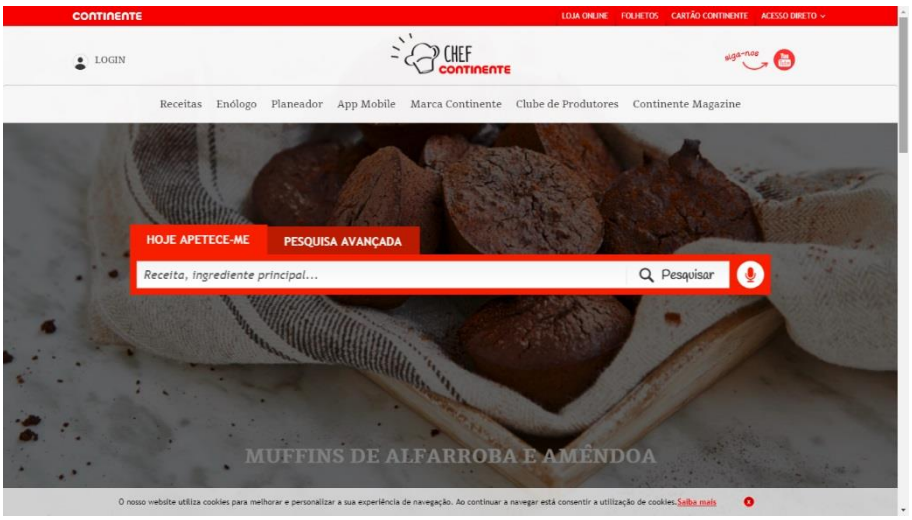

Figure 2 - Chef online landing page

2.1.1 Aries vID Enrolment use case

Identity creation process for eCommerce scenario is currently managed in two ways: the identity could be created on the eCommerce site itself including issuance of credentials, or it could be created using a common identity provider (e.g. Facebook) in which case the eCommerce website will just use the information provided by the Identity Provider. The user is registered to the website during the first login when the identity data received from the Identity Provider are copied into the website users' database.

In both cases the registration process shares a weakness: the identity information (usually private information) is stored in the eCommerce site or IdP databases. In these cases, the privacy threats must be mitigated on the server side of the solution.

In Continente.pt user information is manually entered to the website, it does not contain any verification, only a minimum level of assurance is set. Currently the setting up of the profile is a step that takes time and includes personal data, such as the name and email, and payment details:

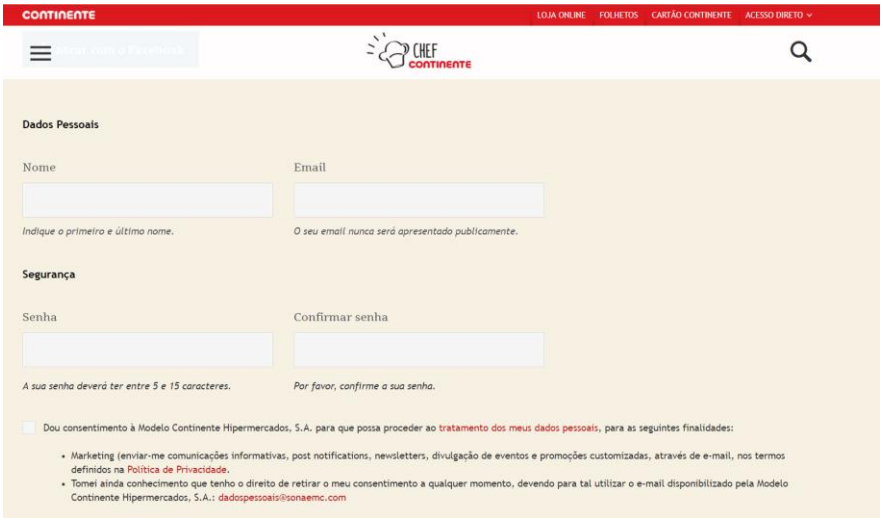

Figure 3 - Sonae Chef Continente Portal registration page

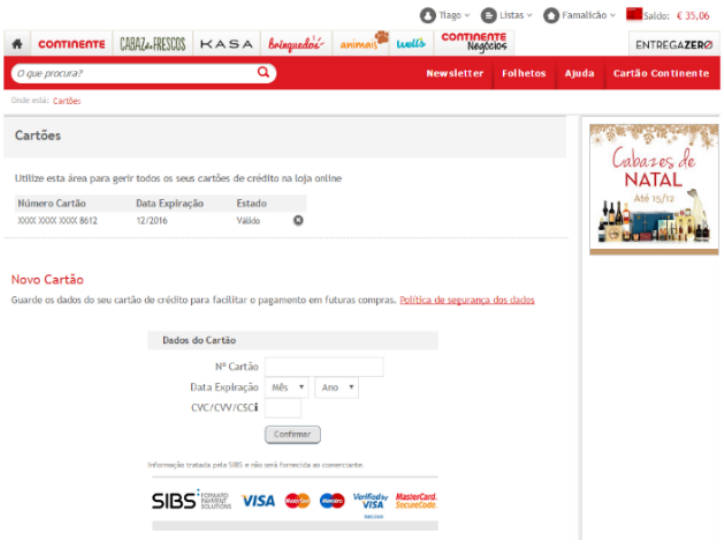

Figure 4 - Sonae eCommerce Portal

The process is implemented as a set of web pages that collect the user information and register credentials.

The proposed ARIES registration process considers that ARIES is going to work in the same way as a conventional Identity Provider: it facilitates authentication data using high level of security credentials and give the user the option to select the attributes to be shared with the eCommerce. Main difference is that those attributes are strongly linked to the user´s credentials and are stored in the ARIES token: they are purged from the virtual ID issuance server. The information must be shared with the eCommerce website, but only

anonymous ARIES ID would be retained by the website, all other information will be used during transactions and purged afterwards.

ARIES enrolment process considers the registration is mobile App centric: the registration started automatically after ARIES authentication App has been installed. The process is simple and only needs an internal app user and identity creation using an official document (passport). The App requires to create self-claimed attributes: attributes not verified with breeder document but containing useful information such as mailing address or email. This provides the same user experience as in the typical scenario.

Aries main added-value:

- User-centric solution with streamlined registration process.
- User can link real physical identity with the Aries vID through the passport this means increased level of assurance of the identity. This may be used in case of some limitations (some goods have age limitation) and lowers risk on eCommerce organization side.
- Additional security enforced by cryptographic means of the ARIES vID token.
- Privacy benefits: user has full control over the personal data. Threat of data stolen from IdP or eCommerce website is lowered.
- Enhanced user experience: the user chooses the attributes to be shared with the eCommerce website with one click.
- ARIES technical approach is underpinned by ethical considerations (EIA). Security and ethics are considered together and in particular in relation to user requirements e.g. deletion of all data when enrolment fails or is cancelled for any reason.

2.1.2 User login and transaction use case

User login use case consists of two steps: verification of user credentials and association of the user identity with existing account.

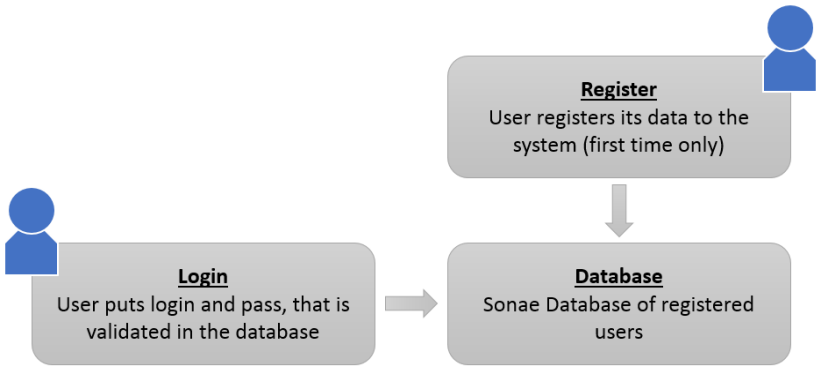

Figure 5 - e-Commerce general login process

The credentials are usually represented by username and password, in more advanced cases an App or mobile handset may be used as credential. In almost all these mobile cases the username is collected as a first step, because it is usually needed to get the phone number for SMS of handset identification for push messages.

ARIES authentication process uses a QR code that removes the need for username submission. This may improve user's perception of privacy and the fact there is no need to remember the username may prove to be beneficial for the user.

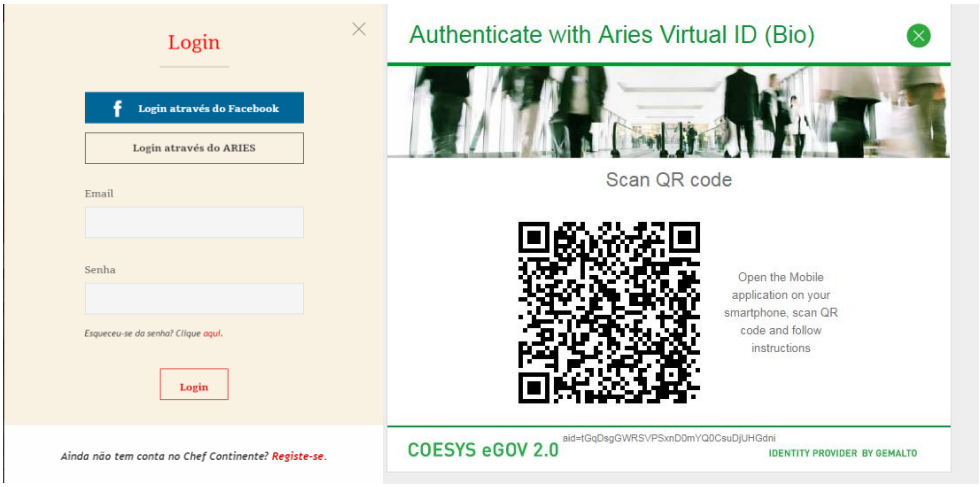

Figure 6 - eCommerce login screens

The typical use case considers simple association between the credentials and the user account information: the username. The data are read from the users' database.

ARIES eCommerce scenario considers usage of pseudonymous ARIES ID as the main user identity. It is an opaque random number, used to link the Aries token with the continente.pt account, and by itself it contains only a little useful information. Additional attributes linked to the ID will be provided by users, they have full control of how much they share with the eCommerce site.

Aries main added-value:

- Additional authentication factor (face biometry) that is usually perceived as strong and difficult to forge.
- Additional security enforced by cryptographic means of the ARIES vID token.
- Minimization of user footprint in the eCommerce systems.
- User has full control over his information.

2.2 *Aries Airport Scenario: Actors and their responsibilities [1]*

Traditional access and boarding control either requires presenting an ID document together with a boarding pass, or when no security assurance is required, is limited to checking a boarding pass without any ID validation. On the one hand, the first case is neither convenient nor efficient because of the need to control a physical ID document. On the other hand, the second case provides no assurance at all to the passenger presenting the boarding pass. In both cases, the control could also be considered as invasion of privacy from the passenger's point of view, since the boarding pass or ID document usually contains more information than what is really needed for the control purposes (e.g. full name, date of birth, flight time and destination, etc.). This becomes even obvious when a boarding pass is presented in airport shops for waiving taxes or for customer analytics.

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

Moreover, ARIES virtual identities can be used to provide a higher level of privacy by just presenting a proof of having a boarding pass, without the need to disclose any other personal data. This demonstrator will show how to obtain a valid ARIES virtual identity and how it can be derived into secondary identities for different purposes.

The overall use case as described in ARIES proposal is summarized by the following figure.

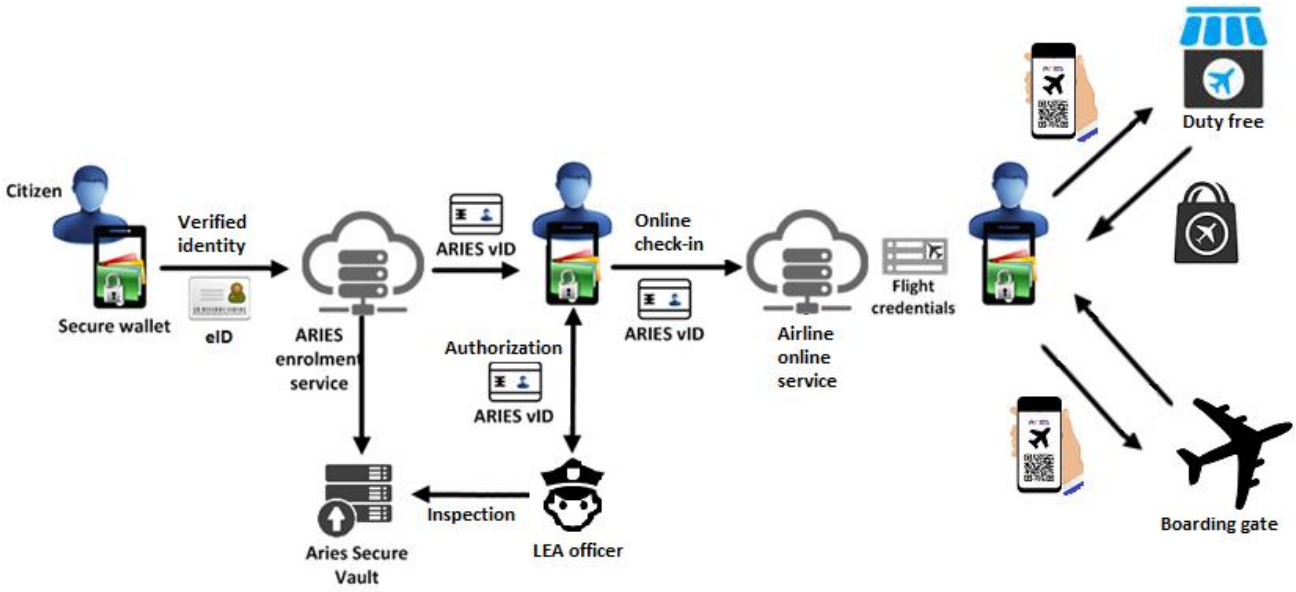

Figure 7 - Airport use case model

Actors

Passenger

The passenger is the person interacting with airport services using a virtual identity, the data subject whose personal data must be protected. The virtual identity is used to prove certain attributes for enabling access to the services.

Identity Provider (IdP)

The identity provider is responsible for issuing the user virtual identities after a preliminary enrolment phase. The enrolment phase will be based on an eID. The IdP encompasses different services such as the Identity proofing service to validate that the user is the genuine person, the biometric enrolment service, as well as the virtual Identity Issuance in charge of generating the virtual IDs.

Service provider (or Relying Party)

The service provider is the one providing the service the user wants to get access to. It could be an online or a physical service. The Service provider in the Airport scenario is going to be embodied by two main entities:

- Duty free Shops → these entities will benefit from ARIES technology, as they will be able to authenticate the user, in a privacy-respecting manner and confirm, during the shopping, that the user has a valid boarding pass in order to comply with the regulations. Passengers will not need to disclose any personal attributes during this operation, only proof that they are in possession of a valid boarding pass. In addition, during the demonstrator, an under-age verification using IDEMIX attributes will be checked.
- Access Control Points→ during the boarding pass control, Jet2 airlines can provide a physical and digital service to validate the ARIES virtual ID, and therefore check whether a person is granted access to security restricted areas. In this demonstrator, the airplane boarding process will be tested. A new boarding pass will be generated using the ARIES virtual ID selected by passenger.

Security Auditor (or LEA officer)

In case of identity theft, LEA officers have the capability of analysing the audit logs of the issuing process and of checking the attributes stored in the secure vault. The secure vault contains the relevant identity information previously generated by ARIES. LEAs can check the physical and virtual identities of citizens in cases where an identity-related crime is reported or when the risk of it happening arises (loss or theft of a mobile device in the airport).

2.2.1 Aries "Boarding control" use case:

ARIES vIDs will help passengers at the airport to:

- Demonstrate, with the highest level of assurance, their real identity at the boarding gate when accessing the plane. That is, passengers have an Aries vID obtained using their passports and they proofed their real identity through biometrics, matching the fresh live capture of the face with the one stored in the chip of the passport.
- Demonstrate they possess a valid boarding pass.
- The authentication process will be evaluated at the airline desk using a mocked boarding terminal system, endowed with a camera and screen. Both ARIES methods, using Mobile vID plus biometric authentication are mandatory (one after the other)

Technical-implementation implications (improvements of the airport ARIES instantiation over the eCommerce instantiation):

- For the biometric authentication, instead of capturing the fresh biometric picture with the user's smartphone camera, the partner in charge of providing the boarding gate simulator will deploy an ARIES embedded system (boarding terminal), able to take the picture in-situ with its own camera and communicate with ARIES identity services. The biometric comparison is performed directly in the boarding gate.
- The boarding terminal scans a QR code presented by the user (in his smartphone), to start triggering the Mobile ID authentication using the Aries vID. In principle, internet connection is needed in the user smartphone to communicate with the ARIES server, optionally WIFI connection provided by the airline could be considered.
- Then, the user shares the biometric token stored in the smartphone in form of QR (obtained during enrolment stage, signed and encrypted by biometric enrolment service), with the biometric verifier service deployed in the boarding terminal (through the ARIES online server). Likewise, during the same session, the terminal obtains a fresh live capture of user's face to perform the biometric comparison with the biometrics used in the enrolment. If comparison is affirmative user is authorized to go into the plane.

Aries added-value:

- Physical document (e.g. passport) is not needed anymore for authentication
- Strong authentication, with highest LoA, based on biometrics
- Human error factor in user authentication and pass verification is minimized
- Stronger self-boarding procedure
- Increased security processes at the boarding gate
- Less staff involved at the boarding gate freeing up staff deployment to other tasks
- Cost reduction which could affect the customer
- Reduced waiting time which should improve performance of airline and airport
- Possibly: preliminary differentiate two different people with the same name through control of the portrait

2.2.2 Aries "Shopping in the airport" use case

In case a passenger wants to buy something in a shop inside the airport, he will need to demonstrate using ARIES vID, in a privacy-preserving way, that:

- He possesses an ARIES vID, that is, he has enrolled in ARIES system, using a legal and valid breeder document, in this case, the passport. The user authenticates through ARIES technology in the shop. Biometrics authentication is not needed since this use case requires a lower level of assurance than the boarding control use case. Authentication using Mobile ID technology is enough.
- The shop assistant will check in a privacy-respectful way, using ARIES, that he is over 18 years old to buy some goods in the shop, e.g. alcohol beverages. This matching age-destination is a must, because majority of age is different in each country. Shops don't need to collect any other information. Aries will comply with the minimal disclosure principle; none other personal attributes will be disclosed.

Aries added-value:

- Privacy-preserving solution:
    - The shop cannot get any user personal info beyond the minimal required information, i.e., only the assurance that he holds a valid boarding pass, the destination and the passenger's age is over 18 (in case of buying certain items)
    - Physical breeder document is not needed anymore to demonstrate the age

Other considerations in the use case that will not be showcased in the Pilot

First, a mechanism for the service provider to specify different LoAs and policies for the authentication process.

Second, users need to demonstrate they have a valid boarding pass. Notice that this step is, in principle, out of the scope of ARIES, as they might still use an existing boarding pass. An option (that will not be showcased) would be to use a token signed by the airline company stating that the passenger has a valid boarding pass, and in this case he would only need to show the QR including the destination information to the shop attendant. Destination is important because some goods can't be sold to passengers flying to domestic destinations (e.g. tobacco, except flying to Canary Islands).

2.3 *Aries "Identity-related cyber-crime" use case*

This use case of identity-related crimes could apply not only to the eCommerce and Airport scenarios, but to any related use case that might be instantiated using ARIES framework. This use case is intended to test the advantages, security and data treatment of the ARIES's secure vault component. The ultimate goal is delegating rights to a third party to access to the user's secure vault and investigate an identity-related cybercrime.

The scenario to showcase is how ARIES can reduce the impact of citizens loss of ID / ID theft. Passengers must report to LEAs the loss of ID documents to formally declare the incident.

Cases of stolen, loss or damaged ID documents need to be immediately addressed to avoid major inconveniences to users and investigations need to be conducted in case of identity theft. ARIES aims to help in such situations.

ARIES envisages to implement, and test internally, when the user has lost his passport:

- Firstly, the user reports the incident, the LEAs and the Aries system are informed about the incident to determine if this is an identity-related crime and to prevent from someone else impersonating the user and generating a new Aries vID using the stolen document. Optionally, a mechanism could be implemented to rise an alert in case the secure vault detects that someone has tried to use the breeder document.

- The LEAs are given rights to look into the Secure vault in order to investigate any identity fraud that could be originated. In this regard, the user needs to confer his consent on his device to enable LEAs to access his information in the Secure vault, including delegation of the proper tokens or credentials to be able to decrypt the personal information stored. The personal information stored in the vault might encompass: correlations among different identifies associated to the user and obtained across different stages (Passport ID, proofing ID, biometric ID, Aries Mobile ID, pseudonyms), authentication logs in the IdP, authentication logs in Biometric Verifiers and previous accesses to the secure vault. It is worth mentioning that the LEA´s grants to access to the vault should be limited in terms of number of accesses and validity time period.

  Nonetheless, it should be noticed that, in principle, the user, for certain kind of flights, could still travel using his Aries vID stored in his smartphone without the e-passport (as theoretically in the future ARIES could replace the ePassport usage for identification).

Aries added-value:

- LEAs can look into the Secure Vault, by checking whether the ARIES vID has been misused in any on-line service.

- ARIES provides means for cyber-crime investigation, LEAs will be able to access valuable information about the user and personal information, which couldn't be performed otherwise.

- ARIES will help LEAs to identify a user without the passport (that has been lost/stolen), using ARIES, thereby facilitating traditional investigation processes.

Other considerations in the use case that will not be showcased in the Pilot:

Although is out of the scope of the Aries Pilots, the procedure for investigating identity-related crimes, applies similarly in any other scenario in which the user reports an identity theft or fraud, such as impersonation. For instance, anyone, including service providers, might report the policy any fraudulent attempt to access a

service. In that case, the user would be warned and notified (e.g. through e-mail), so that he can report the incident to the LEAs, providing them grants to access his information in the secure vault to start investigation.

Passengers might require a temporal physical accreditation document for traveling to some destinations. This accreditation is issued by the LEAs after identifying passengers through different means, interrogating the user, accessing national registers and even accessing international databases. In this regard, ARIES would provide a progress beyond the current state of the art, since will endow LEAs with additional instruments to identify the user face to face, by means of ARIES technology. In this regard, user can employ both, cryptography authentication using his Aries vID stored in the wallet, as well as biometric authentication. This would provide the added value to the safe and secure borders of all countries involved.

3 Prototypes instantiation and set-up

This section describes how each Aries component has been set-up and instantiated for both, eCommerce and Airport scenario's prototypes. The components were implemented in WP3 and more technical information may be found in documentation delivered by the work package.[2]

3.1 *eCommerce scenario prototype setup and instantiation*

3.1.1 Virtual ID issuer

Virtual ID issuer application plays role of the Enrolment web-app: the main orchestration. In the first setup it was a web-portal, but in the final instantiation it was implemented as a pure backend application with REST interface. The UI of the process is supplied by the App.

On the backend the application was integrated with all the other services; all other steps are initiated by the Virtual ID issuer, results are verified and information collected during the process is stored in Secure Vault as the main audit log.

The application was deployed in Gemalto demo environment and made accessible to all other components.

3.1.2 ID Proofing service

The ID proofing service verifies the document genuineness and checks that the user of the smartphone is the one the document has been issued to. In the eCommerce use case, the ID proofing service read data from the ePassport (face image, age, name, document id). In addition, it obtains data from a live capture taken by the smartphone app, and the send to the server for the processing. In the server side, it is checked three main aspects:

- Data signature through passport's PKI
- Data signature through the public key of the issuing authority of the eID document
- Live face capture against the reference portrait extracted from the electronic document

Once the data are verified, they are signed and encrypted by the service and sent back to the client. There is no data persistence in server-side.

The result of the ID Proofing component is a JSON attestation signed and encrypted that contains the identity attributes and the portrait picture.

The ID proofing service composed of several underlying services:

- **The id proofing engine:** that deal with the identity registration policy and the various components and / or external service orchestration
- **The server middleware component** that interacts with the ePassport and verifies the genuineness
- **The biometric matching service** which verifies that the reference document portrait is matching the user requiring the registration
- SDKs integrated within the mobile application

All these services are wrapped by a top-level API server implementing the ARIES API.

3.1.3 Biometric enrolment and authentication service

The biometric enrolment service in the eCommerce use case is integrated with the ID proofing service to get the reference portrait from the ePassport into a Json Web Token signed and encrypted.

The biometric enrolment is in charge of checking the image format (JPEG 2000 for passports), minimum size and quality (brightness, blur, …) and ICAO criteria provided by the ID proofing component by encoding the reference portrait into a face template. If they are acceptable the enrolment is confirmed, otherwise it is rejected.

During the authentication, a matching is done between the face reference template and the live capture. They are wrapped by an API server implementing the ARIES API.

Biometric authentication performs live acquisition of the biometric feature and comparison with the previously prepared information from the biometric enrolment. All the data are used during the authentication and discarded afterwards. There is no additional information acquired in this step.

3.1.4 Issuer service

This service generates new credential for the user. To this aim, the user provides data read from electronic document as well as additional user information (attributes) that he is willing to submit for future convenience. The self-claimed attributes provide lower level of assurance and are treated as such.

Anonymous PKI Issuer service for main demonstrators was implemented as a REST API based web application. The credentials were based on an authentication key pair securely stored in the App and a set of attribute certificates with both proofed and self-claimed certificates. There was a single attribute per certificate to provide the user better control over his personal data.

The issuance considers following inputs:

- PKCS10 Certification request from App.
- JWT with attributes read from the breeder document signed by the ID Proofing service. This information will be used to issue high assurance attributes.
- JWT with attributes submitted by the user (self-claimed attributes). After review of user experience of the first demonstrator we decided to provide this option for user's convenience. Even with low level of assurance the attributes may be delivered to Service Providers so the user does not need to submit them multiple times.

Mentioned JWT attribute request is signed JWT token (by user or ID proofing service) where payload is JSON object containing attributes in key-value format.

As a result of the issuance, the user is provisioned the new virtual ID with following information:

- X.509 certificate issued for private key generated in the App
- Attribute certificates for attributes acquired during the ID Proofing.
- Attribute certificates for self-claimed attributes.

Attribute certificate is signed by vID issuance CA service and contains reference to the holder certificate.

The issuer service receives the input data, processes them and erases them when the issuance is finished. The only persisted information is content of the audit log stored in secure vault.

3.1.5 Verifier service

This service performs the ARIES vID authentication. In our case we selected OpenID Connect protocol as the main means of communication with Service Providers. The protocol is a current state-of-the-art standard and should be accepted by all Service Providers.

The authentication starts with OpenID Connect request from Service Provider to vID Verifier and continues with user's credential verification, attribute reading (both may be done in single step depending on crypto technology used) and then the information is shared with the requesting Service Provider using OpenID Connect protocol tokens. The shared information depends on user consent: the attributes are displayed to the user and he must provide consent and if the sharing is rejected then the information is not submitted even to the vID Verifier.

After the information is submitted to the Service Provider the user loses control over it. Depending on policy the information may consist of: Anonymous or pseudonymous ARIES ID reference, Data read from electronic document and Self-claimed user attributes

The verifier service implementation was based on authentication front-end application supporting SAML 2.0 and OpenID Connect protocols. The application was updated with ARIES authentication method: PKI authentication initiated by QR code reading and deployed in Gemalto demo environment.

3.1.6 Android App

The ARIES App has been developed in Android and provides UI needed to perform all required flows described below. The application is divided in four parts:

a) Home screen. It is the main entry point of the application which includes:
   - User management: interacting with the Mobile Wallet through Virtual ID Manager component to create, rename and delete user´s partitions.
   - User details display: information about all the virtual identities of the selected user and giving the possibility to create, rename and delete them as well.

b) Enrolment. This part is responsible for all the processes related to creation of new ARIES IDs. This process includes:
   - Reading of Passport using ICAO ID Proofing (Section 4.2.1.3[2]
   - Face verification using Facial Recognition SDK.
   - Saving a new Aries virtual identity with all the data generated by the previous described processes during the enrolment step.

c) Authentication. It allows the user to be authenticated in third party's services using Aires Virtual identities which includes simple and biometric authentication (Live Face Recognition). This component uses a QR and Barcode reader library to manage the camera and be able to read the QR code to start the authentication process.

The following components were provided as SDK for Android:

- ARIES vID Manager – main SDK for user information and credential management
- MobileWallet – component for secure storage of user information
- ARIES vID Issuer – SDK for issuance of anonymous PKI credentials
- ARIES Authenticator – SDK for anonymous PKI authentication
- ID Proofing - SDK for document reading and user facial authentication with liveness detection
- Biometric - SDK for biometric enrolment and authentication

The above components have been delivered along with the documentation in Javadoc, the guide for the developers, as well as an example App.

3.1.7 Service provider Web app (Chef Continente webportal)

As part of the eCommerce demonstrator the login and registration into the Continente platform was fully integrated with the ARIES system. This was made by an integration OAuth with the ARIES system consisting of full operability of the processes in the Chef Continente webportal where the registration data were stored in the ARIES vault and linked into the web application, since the authentication process is now delegated to an external entity (ARIES) through the OAuth.

The integration with Service Provider was based on OpenID Connect protocol and since the web portal uses php language a php SDK was provided for smoother integration. The integration was done at the front end (creation of OpenID Connect authentication request) and at the backend to connect to backend of the Verifier service.

The Service Provider in the eCommerce is impersonated by SONAE. A sample implementation has been delivered to test the flow during integration. Besides, a php library was provided to simplify integration with SONAE.

3.2 *Airport scenario prototype setup*

The set-up of the airport demonstrator relies on all the components described above for the eCommerce, plus some additional implementations and modifications to cope with extra requirements of the Airport use case not needed in eCommerce, mainly, the boarding terminal and the duty-free shop terminal.

There is a need to link the virtual identity with the physical access point, the gate, in a way that the physical device could control the identity, to grant (or reject) access to enforce the responsibility of the gate even if the ID document is virtualized.

3.2.1 Boarding use case component's instantiation

In this use case, the idea is to illustrate the different parties:

- The airline application managing the flight related details including the boarding pass
- The ARIES application managing the identity, the privacy related to the identity and the biometry of the user
- The boarding gate enforcing the control of identity between the certified identity and the physical person trying to pass through the gate.

The following additional components were implemented for the airport demonstrator:

3.2.1.1 The airline mobile application

This app could rely upon ARIES to ease boarding by integrating within the boarding pass displayed as QR Code a reference to the biometric template.

In the prototype this is a simple airline app that interacts with the ARIES app and receives back the data structure send by ARIES, adding the flight details and displaying the QR Code.

3.2.1.2 Aries Boarding android app

It is the entry point responsible for handling requests from third party mobile applications. It shares the required data allowing the process of boarding with Aries virtual Identities. There is no specific developed app for the boarding use case, the android app is common for all use cases and all the required implementations are appended to the same app.

3.2.1.3 A boarding gate

The boarding gate is simulated by:

- A document reader scanner (Desko Penta)
- A face matching (Morpho Face) device that is able to acquire the face of the user and match with the template provided to allow or reject the user to go through the gate

To authenticate the user and keep the biometric template private, the QR Code contains a Json Web Token signed with the following information:

- User identity (firstname, lastname)
- Flights details: flight identification, boarding sequence number
- Encrypted face template as biometric data

The boarding API generates the information required to be included within the boarding pass.

3.2.1.4 Issuer Service

In the airport scenario this service is set-up and instantiated in a similar way as in the eCommerce scenario explained in section 3.1.

3.2.1.5 Verifier Service

In the airport scenario this service is set-up and instantiated in a similar way as in the eCommerce scenario explained in section 3.1.

3.2.1.6 Biometric Service

In the airport scenario this service is set-up and instantiated in a similar way as in the eCommerce scenario explained in section 3.1 but it is used, not to register or authenticate a user face, but to encrypt the biometric data (here the face) to be provided to the boarding gate so that it ensures both confidentiality and compatibility

3.2.1.7 ID Proofing based on Spanish eID

In addition to the ID proofing service based on ePassport, the Airport demonstrator also integrates the ID proofing based on Spanish eID to provide the possibility of using the official National Document of Identification issued by Spanish authorities, namely DNIe v3.0, in the ID Proofing service.

Note although this module is tested during the airport demonstrator, it was developed as part of the enrolment process at the beginning of the project, and it is a core element of the ARIES platform.

This module has several internal components:

- OCR: this component reads the MRZ characters of the DNIe document. These data will be used to create a secure NFC channel between the mobile device and the physical smart card. To do that, this module manages the built-in camera in the device.

- JMRTD library with NFC: in the case of this component, it is used the open source jMRTD library to open a NFC channel using Basic Access Control (BAC) protocol and enable the mobile device to obtain the required information from the ID document, i.e. personal data and face image.
- Transfer: it provides the base proofing interface to communicate with the ID proofing service. The complete workflow of this module can be described as it obtains the required personal data from the DNIe, signs all the information using JWT standard RFC 7519 and finally sends all to the ID proofing module.

3.2.2 Duty-free shop use case, component's instantiation

The instantiation of this use case assumes some considerations:

- The connectivity between the mobile and terminal is done over WIFI.
- The boarding pass verification is done as in the boarding use case.
- The Aries app obtains certified attributes. Aries Proofing is done from ePassport.
- The mobile sends the user's photo to the terminal, which verifies the photo validity (signature) and shows the photo to the shop assistant in the screen of the shop terminal.

In addition to the component instantiation of the boarding use case defined in previous section, three additional components are needed to cope with this use case:

3.2.2.1 Idemix Issuer service

It generates Idemix credentials based on Aries vID and checks the signatures. The Idemix credentials are stored by the user in his smartphone in a special purpose mobile wallet.

3.2.2.2 The duty-free shop terminal:

It deploys an Idemix Verifier service in charge of verifying idemix proofs presented by the user mobile app. Namely a crypto proof that demonstrates he is over 18 years old. In addition, it verifies and shows to the shop assistant the user photo (to provide higher level of assurance).

3.2.2.3 Extended Aries app

The ARIES app has been enhanced to integrate the Idemix user android library, which plays the role of attribute prover and recipient of Idemix credentials delivered by the Idemix Issuer service. The app also holds a mobile wallet to keep the Idemix credentials and related user-secrets.

References

[1] D3.1 ARIES eID ecosystem technical design

[2] D3.2 Virtual identity developments