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

ARIES
"reliAble euRopean Identity EcoSystem"

D4.5 – Evaluation and Validation Report

Due date of deliverable: 28-02-2019
Actual submission date: 28-02-2019

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 HORIZON 2020	
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	

D4.5 – Evaluation and Validation Report

Editor
Martin David (GTO)

Contributors
Javier Presa (Atos)
Stuart Martin (POCC)
Sebastien Bahloul (Idemia)
Julián Valero (UMU)
Jorge Bernal Bernabe (UMU)
Tiago Costa Oliveira (SONAE)
Dave Fortune (SAHER)

Reviewers
IDEMIA
UMU

27-02-2019
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	15/01/2019	Martin David	ToC
0.2	22/01/2019	Martin David	First draft. All sections.
0.3	29/01/2019	Javier Presa	Section 2.2
0.4	31/01/2019	Javier Presa	Update on section 5
0.5	01/02/2019	SAHER	Chapter 4
0.6	02/02/2019	Julián Valero /Ignacio Alamillo	Sections 2.1.2 and 3
0.7	11/02/2019	Martin David	All sections
0.8	15/02/2019	Stuart Martin Tiago Costa	Section 5.3 & 5.4
0.9	18/02/2019	Sébastien Bahloul	Sections 2.3, 2.4 & 5.1
0.10	19/02/2019	Martin David	Review all sections. Conclusion
0.11	25/02/2019	Sébastien Bahloul	Section 2.3.2
0.12	25/02/2019	Martin David	Final review
1.0	27/02/2019	Javier Presa	Final version

Executive Summary

This document is an evaluation of Aries H2020 project. The project goal is to provide a framework to deliver privacy friendly virtual identity cryptographically derived from electronic document with a specific aim to tangibly achieve a reduction in levels of identity theft, fraud and associated crimes. The goal was approached in several steps: requirement definition, architecture design and pilot implementation.

Technical aspects of the project are evaluated at two levels: evaluation of architecture with remaining points that must be implemented by each solution instances and evaluation of pilot implementation.

The dataflow analysis provides a clear view of all flows involving personal data (including biometry) and sets a security and privacy baseline a minimal level that would be achieved by every implementation project regardless on technology used. This can be considered an advancement of state of the art in comparison with existing solutions. There are several security risks that cannot be addressed on architecture level must be addressed by each implementation and this document provides implementation recommendations. Pilot implementation addressed the points is a sufficient yet minimal way in line with expectations.

From scalability and performance point of view the architecture does not introduce any bottlenecks and deployments up to several millions of users should be possible. Of course, each component may have its own hardware requirements, but the architecture allows each of them to scale at required velocity without impact on rest of the system.

Future expansion and reactivity to new technologies is ensured by the fact that the architecture defines a framework of components, but not any protocol or other constraint. This ensures new authentication methods, biometric verifications and cryptographic schemes may be introduced in future and the both the new and the legacy may be used together (e.g. when the feature is available to users of selected handsets). This flexibility was demonstrated by pilot implementation of voice authentication leveraging on existing authentication server that was inserted into the solution using only a lightweight proxy server enriching the authentication with Aries required features.

This document provides a comprehensible evaluation of coverage of requirements collected in WP1 and WP2: functional, non-functional, legal and ethical requirements. The analysis provided a clear result: the project architecture framework provides good guidelines, but on their own they don’t ensure that all requirements are fulfilled. There are many that must be addressed by organization process such as audits, reviews and communication, the real compliancy depends on each implementation.

Pilot implementation covered most of the requirements with following exceptions:

- ID Recovery use case was not implemented. This use case provided a good functionality for the user, but at the same time it also limited privacy as it was mandatory to store part of the identity on the server side.
- There was no organizational setup for pilot.
- Standard protection of data on server side was limited (data encryption, secure calculations using HSM).
- Privacy was not perfect as one architectural component (Privacy proxy) was not included in pilot. This component has no impact on user experience or any part of the evaluation.
- Identity federation was not selected for pilots.

The feedback collected from pilots was in general positive and addressed points expected for prototype projects:

- Users would appreciate iOS support.
- More optimizations of the user experience were recommended including guidance through the processes, more detailed help and better feedback in case of errors.

- Optimization of the boarding process mainly of the boarding terminal to improve throughput.
- Better integration with airline companies to provide more streamlined process of boarding pass issuance.

Contents

List of Figures

List of Tables

1 Introduction

This document presents evaluation of Aries project results. Goal is to evaluate outcomes in relation to inputs of the project and to provide recommendations for project users regarding policies and end-user processes.

1.1 *Relation to other project work*

This document is a deliverable of task T4.5 of work package 4.

Inputs for project evaluation come from three work packages:

- **WP2 Procedural, ethical, legal & societal requirements for ID ecosystem:** this work package provided requirements for project specification and implementation and main goal is to verify and provide evidence the requirements have been covered.
- **WP3 - Strengthening the technology for ID:** main technical work package providing technological background for pilots. This WP provides technical documents and component implementations to be assessed against the requirements.
- **WP4 - Demonstrators Integration and Evaluation:** all pilots were part of this work package, input for evaluation are pilot results in form of documents and user survey results.

1.2 *Structure of the document*

The evaluation is split by topics and each topic is covered by a separate chapter:

- **Chapter 2**: Technical evaluation is based on Aries architecture design and implementation provided by WP3. From technical point of view, it is evaluated in several steps: dataflow analysis, security, privacy and GDPR, requirement compliancy, performance and sustainability.
- **Chapter 3**: Legal evaluation and compliancy to legal requirements
- **Chapter 4**: Socio-ethical evaluation
- **Chapter 5**: Is a compilation and analysis of all information collected during the pilot including feedback from integration and improvement points.
- **Chapter 6**: Conclusions and recommendations for exploitation and future extension of the project

1.3 *Glossary adopted in this document*

This document uses the same terminology adopted in the project.

1.4 *Acronyms used in this document*

eID	Electronic identity
eIDAS	electronic IDentification, Authentication and trust Services
GDPR	General Data Protection Regulation
IdM	Identity management application
LEA	Law enforcement authority
MRZ	Machine readable zone
NFC	Near field communication
OTP	One type password
PIN	Personal identification number
PKI	Public key infrastructure
T	Task of ARIES project
TLS	Transport layer security
SAML	Security assertion markup language
SDK	Software development kit
SP	Service Provider

UI	User interface
vID	Virtual ID
WP	Work package of ARIES project

2 Technical evaluation

This chapter provides evaluation of all technical aspects of the project and is based on design documentation and developed components.

2.1 *Security and privacy evaluation*

Security and privacy are two the most important aspects of the project as the main goal is to provide more security for the end-user namely to address the most frequent security threats and to follow privacy by design principle.

The security of the solution may be assessed on the basis of the architecture definition, but the security and privacy of each instance strongly depends on the implementation. The project does not provide exact blueprint of how to implement each component but rather a guideline how to bind the components together. Privacy also depends on the process deployed on top of the solution: segregation of the components and physical measures taken to ensure the solution is not vulnerable to rogue administrators and other insider attacks. This analysis takes all of this inputs in the account and provides evaluation for all these cases.

2.1.1 Dataflow analysis

This analysis is a complete dataflow analysis of the Aries solution with all variants that may happen as long as the architecture concept is followed.

2.1.1.1 List of private information in the system

Reference	Type	Origin	Destination	Persisted where
eDocument data	Information read from electronic document: user attributes (date of birth, gender, photo)	Electronic document	ID Proofing server	Transient
Processed eDocument data	Cryptographically processed information from document (signed).	ID Proofing server	Mobile App	Mobile Wallet
Biometric data	Information needed for enrolment of biometric credentials	Live capture by App	Biometric enrolment	Transient
Processed biometric data	Processed biometric information, biometric credential	Biometric enrolment	Mobile App	Mobile Wallet and/or Biometric enrolment
Credential issuance input	Inputs needed to issue vID credentials such as public keys, prime number sets etc.	Mobile Wallet	vID Issuer	Transient
Credential issuance output	Output of issuance process such as certificates.	vID Issuer	Mobile Wallet	Mobile Wallet
Identity references	Anonymous references of each credentials. Together they bind all issued credentials together.	Biometric enrolment, vID Issuer	vID Issuer	vID Issuer
Biometric authentication information	Information exchanged between App and Biometric verifier server. Definition of this information is out of scope of Aries architecture. Security analysis will be done for following: - Live capture and processed biometric data - Result of processing of live capture and processed biometric data	Mobile App	Biometric verifier	Transient

Aries authentication information	Information exchanged between App and Identity verifier. Definition of this information is out of scope of Aries architecture.	Mobile App	vID verifier	Transient
Information about Service Provider usage	Information in authentication request of eCommerce scenario	Service Provider	vID verifier	Transient
Authentication transactions	Information about authentication (Identity references, SP, time, IP address and other)	Identity Verifier	Secure Vault	Secure Vault

Table 1: Private information in ARIES system

2.1.1.2 Issuance flow

During issuance user information is collected and combined into a single Aries vID. The architecture defines only control part of the flow, the details of each step are up to each vendor to define.

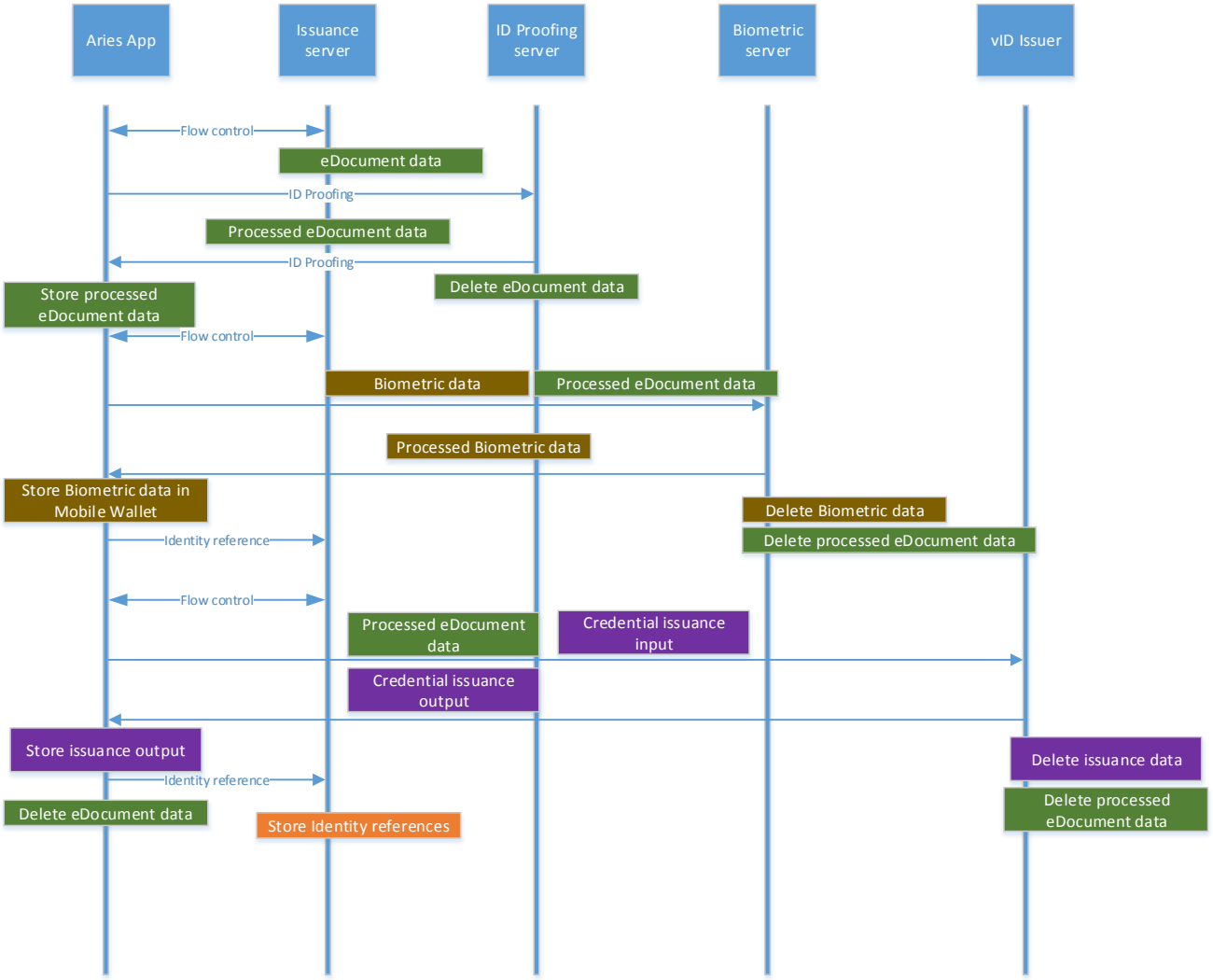

Figure 1 - Issuance data flow

The issuance flow starts with the ID Proofing step where the information read from electronic document is exchanged with the server and cryptogram with proof of validity is created by the server and stored in the App (Mobile Wallet). The real information exchanged strongly depends on implementation by the vendor. The ID Proofing may be split between the App (ID Proofing SDK) and the server. It may vary from version where the data are read by the SDK, formatted and sent to the server in thick client SDK to version where the data are read by the server directly (using SDK as a thin proxy similar to NFC reader). The data should be at least partially verified by the server (Passive authentication and Active authentication in case of ICAO passport) to mitigate identity forgery. The scope of verification must be clearly defined and made available for audits.

The ID Proofing server processes the data and creates tokens used as identity claims for the issuance process. The claims may take any form, but it must provide integrity and authenticity protection in form of digital signature. Trust must be established between the ID Proofing service and vID Issuer. If the authenticity protection is weak then the attackers may be able to issue vID based on forged eDocument information.

The ID Proofing step is the weakest point of the whole process as at this stage the server holds the full identity information: name, date of birth and other attributes together with face image. The data read from the document must be deleted after the ID Proofing is finished and possible software audits should be enforced to ensure it is done so, because this step does not provide any protection against insider attacks (rogue administrators with access to the servers).

The biometric enrolment may be implemented as two main options: enrolment based on ID Proofing data (to ensure link between vID and electronic document) and enrolment of additional biometric type with no information from ID Proofing (for multimodal authentication such as voice recognition).

The enrolment with ID Proofing bio data considers usage of previously obtained and processed information from the document and live capture. The data are transmitted to the Biometric server, processed and new information is created: Processed biometric data. The data format is proprietary to the Biometric server vendor, but need to be stored securely in the Mobile Wallet. At the point the Biometric server holds following information: anonymous identity reference and biometric data belonging to it. It means that even in case of insider attack the threat is limited as the attacker would only get hold of anonymized data and without additional information (that is stored in separate components) he would not be able to associate it with user identities. Recommendation of the project is to make all biometric processing transient and to store biometric information only in the Mobile Wallet, but even if this recommendation is lower the threat is not high.

The enrolment of additional biometric modus is the same as the ID Proofed biometric case, but the information shared with the server is even more limited, because it contains only live capture data.

The issuance of the vID considers usage of personal information obtained from the document to issue attributes for authentication. This information is processed and resulting credentials are stored in Mobile Wallet. At the processing time the issuer has both attribute information and identity part reference which means for some cryptographic schemes the issuer may be able to compromise the privacy. This is the case of PKI based approach used in pilot. In this case there must be a process deployed to audit the application to ensure the information is treated securely and purged after the processing is finished. Note that it is not the case for the anonymous IDEMIX credentials.

There are several security risks to the issuance process:

- ID Proofing impersonation risk depends on strength of the ID Proofing comparison of the live capture and information from the document.
- Data leaks during the communication (eavesdropping) may be mitigated by transport level security with man-in-the-middle attack protections.
- Session theft risk (attacker waits for the user to finish ID Proofing and then takes over the process) depends on communication vulnerabilities and may be mitigated at transport level (certificate pinning, securely stored session keys and other).

2.1.1.3 Authentication flow

Authentication happens in one vID verification steps and zero to multiple biometric verification steps. The exchanged data may vary as the algorithm details are out of scope of Aries project design.

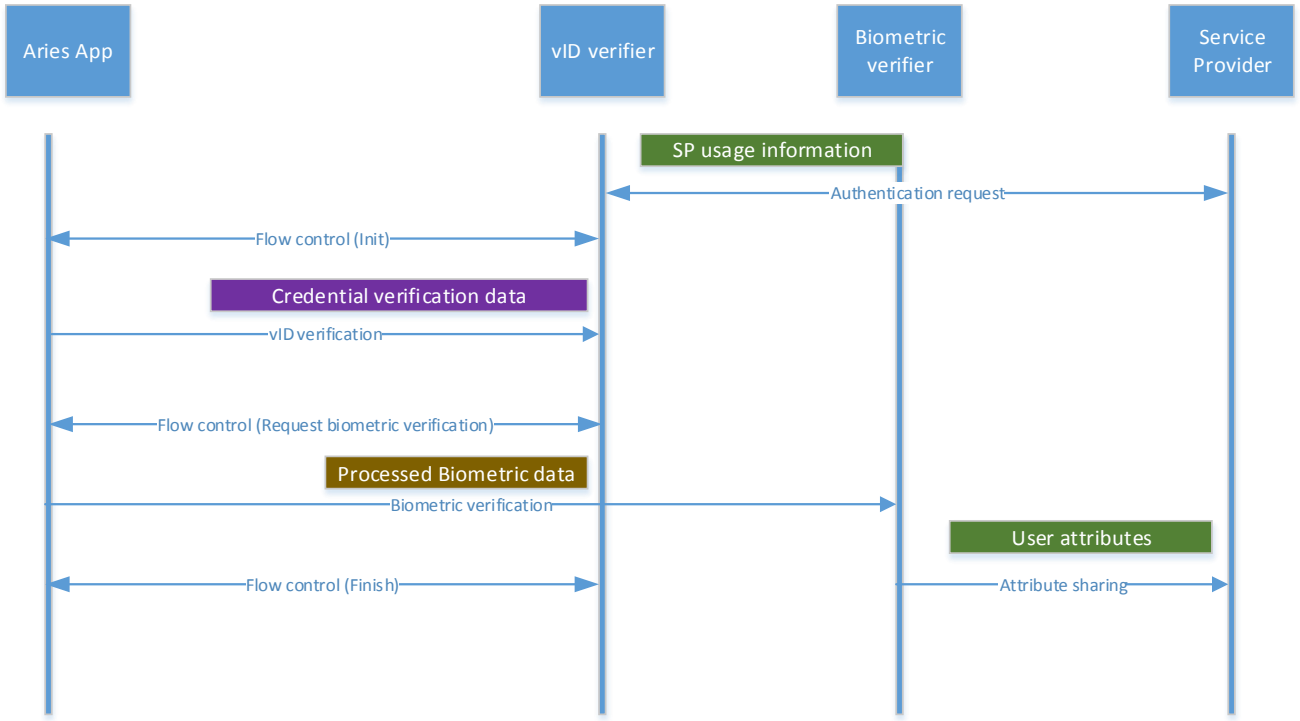

Figure 2 - Authentication dataflow

Authentication starts with Service Provider requesting the verification and information the user uses this particular Service Provider must be considered personal. In the architecture it is noted that this information must be protected from the verified using a proxy or similar measure.

The authentication flow is started by vID verifier: an application in charge of vID verification and flow control at the same time.

The vID verification is done as the first step and level of personal information shared varies depending on cryptographic scheme used:

- In case of PKI related flows, the user provides digital signature and a certificate
- In case of OTP or similar shared secret scheme the user provides identifier and one-time secret generated by the App
- In case of zero knowledge proof flow the verification consists of few steps to provide requested attribute without disclosing any unnecessary information that may allow user tracking

Biometric verification is done after the vID verification was successful and the architecture allows multimodal biometric authentication when the verification is implemented as a set of independent verifications.

The data exchanged during biometric verification strongly depend on implementation. In cases the biometric enrolment results in cryptographic credential protected by local biometric verification the information shared is anonymous and does not contain any biometric data. In cases the verification is partially or fully done by the Biometric verifier the exchanged information must contain processed biometric data and also live capture data and of course must be protected accordingly. Note that Aries project provided architectural recommendation the biometric information should not be stored on server side.

The authentication finishes with attribute sharing between the vID verifier and the Service Provider. The information shared may vary from minimalistic attributes (such as user is older than 18 years) to providing also permanent pseudonym of the user that would allow linking of the user and existing account in Service Provider application. This depends on contract between the Service Provider, vID verifier and the user, but may be heavily constrained by the verification scheme: if the scheme provides minimal information then the vID cannot disclose more to the Service Provider.

The authentication flow shares same security risks with the classical web authentication flows:

- Session theft (after the authentication is finished)
- Information leaks on Service Provider side
- Credential forging risk strongly depends on security of the App and the cryptographic scheme. Aries architecture in this case provides more security in case the implementation of the Mobile Wallet is strong enough.

One specific risk comes from the decoupling of the vID verification and biometric authentication. In case the attacker steals the session and performs biometric authentication with a different device he may be able to mislead the vID verifier (both verifications are correct, but both of them were done for a different user). The protocol to bind the steps and measures how to bind the credentials are out of scope of Aries design, but are one of the most sensitive parts of the implementation of each Aries instance.

2.1.1.4 Airport verification flow

Airport verification flow utilizes Aries vID verification with subsequent biometric verification that is done at the side of the boarding gate to ensure the verification is done by trusted component.

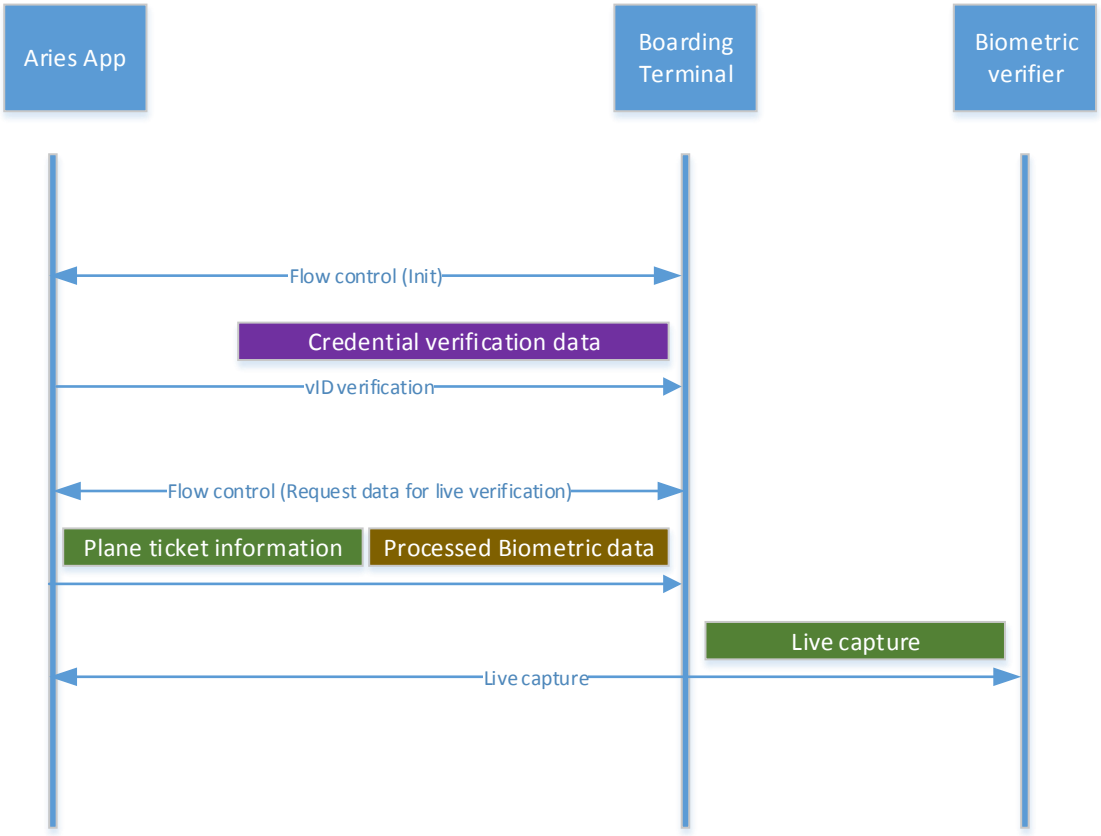

Figure 3 - Airport verification data flow

The first step is vID verification 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 should perform the same verification as in the online case. The live capture information must be used and discarded after the whole process is finished.

The boarding use case brings additional risk of relaying attack. The user standing in front of the boarding gate may have an attacker App that instead of performing the authentication relays the messages to real App or attacker device. This may be used for protocol attacks as well as impersonation attacks, but since the system performs verification of live capture (and the attacker cannot replace the one standing at the gate) the risk is mitigated and depends on strength of biometric comparison of live capture vs. the processed biometric data.

2.1.1.5 Conclusions

The security and privacy of the Aries use cases depends on actual implementation of each block, but the architecture design provides a constraint, a minimal level of security and privacy the solution must provide. Privacy and resistance to insider originated attacks (e.g. database data theft) strongly depends on level of segregation. In case the whole solution is deployed by one monolithic organization the threat of insider attack is significantly higher. The fact the system is modular is not only useful from deployment point of view (to utilize existing systems) but is also an ideal operation model. When the solution is deployed by a single organization the segregation of each service should be enforced by process rules.

The system also provides enough information for crime investigation by LEA and the information is stored in Secure Vault. The architecture requires there is a strong access control mechanism enforced on this component but does not define how it is done. It may vary from a regular database-like engine with strong authentication, authorization and audit logging (which provides minimum, but still is not enough for privacy by design approach) to a cryptographically protected storage where all the information is encrypted by user-controlled key (stored in Aries App or in a cloud protected by Aries authentication).

2.1.1.6 Security measures deployed in pilot implementation

Implementation path selected for pilot considered above mentioned risks and provided following countermeasures.

Risk	Countermeasure	Remarks
ID Proofing impersonation	Limited by deployment of advanced biometric comparison algorithms.	
Data leaks during the communication	TLS with optional certificate pinning	
Session theft risk	Session ID of sufficient length and entropy.	In production probably should be improved by deployment of additional session protection keys or other mechanism.
Information leaks on Service Provider side	Not in scope of Aries.	Must be a part of SP enrolment process (e.g. audit).
Credential forging	Pilot implementation used PKI with state of the art cryptographic strength.	

Table 2: Security measures deployed in pilots' implementation

2.1.2 Privacy and GDPR compliancy

An exhaustive analysis on how the diverse components of ARIES ecosystem treats personal data and its compliance to GDPR provisions was already made with the Data Protection Privacy Impact Assessments (DPIA) carried out in deliverable D2.4 (*Privacy and data protection compliance report*). Therefore, the following table only presents the assessment of the legal conditions on data protection issues as they were described in the Annex of deliverable D2.3 [1]

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
P-1	Privacy	The ARIES provider shall make an inventory of all the specific purposes for which personal data are going to be processed by ARIES	Fully	The Aries Provider describes the purposes for which the personal data is going to be processed.
P-2	Privacy	Personal data can only be linked to a concrete user during the period required by those purposes	Fully	Personal data can be linked to users only in secure vault, after user consent, and in case the inspection grounds are met, in case of identity theft/crime. In the personal data in IdP is kept pseudonymized. The Idp does not store any personal information, the data is kept securely protected in user secure wallet (inside mobile), and it is removed when the app is uninstalled, or whenever upon user request.
P-3	Privacy	The users have to be informed about GDPR requirements regarding the data processing.	Fully	The Aries MobileApp informs users and the users accepts the terms and conditions.
P-4	Privacy	The use of biometric data requires the explicit consent of the data subject for identification purposes	Fully	User are requested explicit consent and awareness, for identification purposes when it comes to biometric data.
P-5	Privacy	The consent must be recorded in a proper way in order to answer a user's claim or to face an inspection from a supervisory authority.	Fully	At architectural level it has been documented. However, it has not been implemented in the Pilot, as it is out of the scope.
P4	Privacy	An easy way for withdrawing their consent has to be offered to the users and the date of this action has to be registered.	Fully	Users can, at any time, remove any identity-related information a personal data hold inside the Aries Mobile App. Future service providers (SP) adopting ARIES would needs to enforce this consent withdrawal, which is out of the scope of ARIES.
P5	Privacy	A concise, transparent, intelligible and easily accessible form, using clear and plain language is offered by the ARIES provider in order to allow users to exercise their rights.	Fully	The form has been offered to the users also providing an email address to exercise their rights
P6	Privacy	The ARIES provider allows users' access to their own data in a structured, commonly used and machine-readable format.	Fully	Users can employ ARIES Mobile App to access to their personal data in a user-friendly way.
P7	Privacy	The ARIES provider has created a record of processing activities. With adequate security measures.	Fully	The Aries secure vault can record correlations between different pseudonyms, employed by users in different contexts. That information is kept protected (encrypted) in the secure vault.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
P8	Privacy	Pseudonymisation criteria have been applied to the processing operations.	Fully	Virtual identities assigned to users are pseudonymized, so that their real identity cannot be inferred.
P9	Privacy	There is a way to re-identify the user in order to make the information available to a competent public authority	Fully	The secure vault contains the correlations between different identifies and pseudonyms given to the user in different context, in order to re-identify the user.
P10	Privacy	By default, only personal data necessary for each specific purpose will be processed	Fully	Only the minimal amount of personal information is released to the Service provider. Using anonymous credentials systems, that allows revealing proofs of having certain attributes, even without disclosing the attributes values.
P11	Privacy	For the airport scenario, the use of Passenger Name Record (PNR) has been restricted to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes	N/A	The PNR information has not been used in the ARIES Pilot.

Table 3: Privacy requirements compliance matrix

2.2 *Requirement compliancy*

In order to analyse the compliance of the requirements defined in the initial phase of the project and reflect how they are linked to the system architectural design, the following table presents the description of such requirements and their implementation in the ARIES platform.

The information of the requirements is extracted from previous submitted deliverable D2.1 [2] and is distributed in functionals (eCommerce and airport scenarios) and non-functionals based on the nature of the requirement.

2.2.1 Functional requirements

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
E 1	Functional	The login procedure should be intuitive and straightforward to accomplish, allowing for a good customer experience.	Fully	eCommerce website provides a button to login with social network or with ARIES. In case of ARIES, the website presents a QR code to be read by ARIES app.
E 2	Functional	ARIES should provide user friendly website and mobile apps, with intuitive user interface and experience	Fully	eCommerce website is hosted in a known webpage provided by SONAE. The mobile app contains the needed screen and minimize the use of clicks for the identity enrolment and usage.
E 3	Functional	The system should support authentication based on at least with a biometric characteristics, such as the fingerprint, face	Fully	Not only for authentication but for enrolment face recognition and voice recognition is implemented on the app.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
		recognition, iris recognition or voice recognition		
E 4	Functional	Customer should be able to login and logout through authentication of the ARIES vID linked to a customer ID	Fully	The authentication process of the ARIES vID is coupled to the login process,
E 5	Functional	The system should provide means for profile creation/update. Including update customer information, such as, for example, name, phone number, fiscal number, gender, birth date, family details, address, credit card number, Continente Card number (loyalty card)	Fully	In the ARIES app, during the enrolment process, it is possible to include self-claimed attributes linked to the vID
E 6	Functional	The ARIES Identity Provider should provide means for validating the user ID to the eCommerce website, so that the user can be identified univocally.	Fully	Every time the eCommerce website requires the identity of the user, generates a new unique token identity.
E 7	Functional	The eCommerce website should incorporate the authentication client to interact securely with the Aries authentication service.	Fully	eCommerce web page displays the option to use ARIES as an authentication service that is triggered by authentication client of the website
E 8	Functional	The authentication service of the Aries ecosystem should provide reliable means for verification of user's identities.	Fully	ARIES app is provided with biometric verification, with linkage to the vID of each user
E 9	Functional	Authentication can be done using biometrics, so that strong and secure identification is provided and the user experience is much simpler.	Fully	ARIES app uses the face recognition and voice recognition for authentication
E 10	Functional	The ARIES IdM should keep user's personal data accessible only for authenticated users (to the Wallet).	Fully	The personal data is securely stored in the wallet and password protected for each user
E 11	Functional	Newer European Commission law/regulation about data privacy must be respected.	Fully	ARIES app is GDPR compliant
E 12	Functional	Authentication through login-password should be avoided.	Fully	Following the authentication flow of the ARIES app, it is mandatory to use biometric in during authentication process.
E 13	Functional	The Aries IdP should validate the biometrical data	Fully	The verification of the biometric is done in the ARIES server with no other connection

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
E 14	Functional	Federation might be used for cross-border authentication, as described in eIDAS.	Partially	Architecture allows it, but this use case was not demonstrated in pilot.
E 15	Functional	The Aries must implement pseudonymous authentication	Fully	Once the user is authenticated, the shared data with service provider is pseudonymised
E 16	Functional	The Aries should implement anonymous authentication with attributes of high level of assurance	Fully	The authentication service provides anonymised authentication (via token) and using attributes obtained from the document reading process.
E 17	Functional	User consent must be requested each time private information is shared	Fully	The user consent is requested during the attribute sharing process.
E 18	Functional	The Aries should allow handset sharing: it must allow multiple users sharing the same handset for their eCommerce activities with their private information protected by separate credentials.	Fully	Multiple users can be enrolled in the same handset. Those are secure stored in the wallet separately and password protected.
E 19	Functional	The Aries must provide authentication service to eCommerce organizations using well known standards to ensure smooth integration.	Fully	The architecture is in line and it is proven by eCommerce pilot, integrated with SONAE website using Open ID Connect protocol (using php SDK).
A 1	Functional	User should be able to create and manage virtual identities	Fully	ARIES contains the virtual identity issuer for providing a vID linked to official document
A 2	Functional	User should be able to make use of their virtual identities against different services provided by different service providers.	Fully	ARIES architecture allows usage of different identities that provide selected information of the user depending on the service providers necessities.
A 3	Functional	Virtual identity allows to demonstrate one or more user's attributes	Fully	With the help of the vID Authentication Client, ARIES app provides the possibility of selection of user attributes
A 4	Functional	The attributes revealed to the SP should depend on particular policies.	Fully	It is on the user decision the selection of the attributes to be shared with the SP
A 5	Functional	The service provider must request the user to authenticate himself/herself with respect to the presented vID	Fully	The service providers present a request (QR code) with the information of the required vID to be authenticated
A 6	Functional	User should be making enrolment in the IdM prior generating the virtual Identities	Fully	It is not possible to access the vID generation or selection if the enrolment is not done in advance
A 7	Functional	Virtual identities should be kept cryptographically protected in the smartphone (in the wallet)	Fully	The wallet is in charge of safe storage of user data and it is encrypted
A 8	Functional	Virtual identities should be securely derived by means of a highly secure process from physical official identity/travel	Fully	The virtual identity issuer is in charge of binding ID proofing based on official breeder document and biometric verification transactions to a new virtual ID

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
		documents (which have been issued under strict assurance conditions by authorized entities)		
A 9	Functional	Virtual identities are univocally bound to source document and person, non-transferrable and must be securely verified	Fully	Biometric Verifier service ensures the authentication of the mobile owner, by comparing the biometric data of the virtual identity with a live captured data.
A 10	Functional	Mobile virtual identities should be linked to the physical travel/identity document	Fully	ARIES App architecture provides the breeder document verifier as the implementation of the physical document verification.
A 11	Functional	Virtual identities could be used to present a proof of having a boarding pass, without need to disclose any other personal data	Fully	The usage of virtual identities that may disclose only selected attributes of the user could be used, for example, to display the boarding pass without disclosure of name or birthdate.
A 12	Functional	A security procedure and mechanism for storage of identity related information (such as IDs correlation) should be provided (in the security vault)	Fully	The vault is storing data encrypted within the vault. Only the user as authenticated by the VID component could get access to it, and an escrow key that allows Law Enforcement Agents to get access to data according to local legal framework.
A 13	Functional	A security procedure to log data on enrolment/issuing process should be provided (security vault)	Fully	Architecture compliant and in pilot implemented using secure Syslog in secure vault.
A 14	Functional	The security vault logs might be checked only under specific circumstances e.g. Identity-related crime	Fully	The interface to the Secure Vault implements secure communication, strong authentication and authorization mechanisms.
A 15	Functional	The security vault could be used as a repository to provide more assurance or to complement information about attributes available within the virtual ID for the attributes verified during the ID proofing - not the one self-claimed by the user.	Fully	The Secure vault will store and properly protect attributes from the user enrolled in ARIES to provide more assurance or to complement attributes available within the virtual ID.
A 16	Functional	Security vault should provide confidentiality, integrity, access control protection and audit trails.	Fully	The secured storage with web service API provides reading and writing functions and confidentiality, integrity, access control based on user consent via ARIES app and logging data process on enrolment/issuing process.
A 17	Functional	A subject (User) should be able to demonstrate the link between its legal ID and the virtual ID a user of a service has.	Fully	The attributes obtained from the breeder document are the basis of the virtual ID of a user and they are directly linked to such document. In addition, the link between breeder document and the token will be only stored in audit trail in Secure Vault
A 18	Functional	The access to the wallet data should be performed only after a successful user authentication	Fully	In ARIES App, there is a Credential Manager that works as a firewall between authentication and Secure Wallet.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
A 19	Functional	Different authentication factors might be provided	Fully	Face recognition and voice recognition are available as authentication factors in the ARIES app
A 20	Functional	The police should be able to check the secure vault after user consent	Fully	The ARIES mobile app will provide an authentication token through its request to access the security vault.
A 21	Functional	User should be able to employ ARIES IdM ecosystem for shopping in the airport	Fully	The use case of duty free is implemented in the ARIES app, allowing the user to share attributes using zero-knowledge proof.
A 22	Functional	User should be able to employ ARIES IdM ecosystem for boarding	Fully	The use case of boarding is implemented in ARIES app, allowing the user to use the vID to generate a boarding pass with the personal information embedded.
A 23	Functional	The IdP should not maintain user biometric information. The IdP should only use biometric information for user authentication without storing the user raw biometric data.	Fully	Biometric Enrolment service stores the biometric data captured during ID proofing event within the mobile app in the secure wallet, but this service does not maintain any user's biometric data in the server-side.
A 24	Functional	vIDs should not contain revealed or raw biometric data.	Fully	After the biometric enrolment, a proofed identifier (biometric ID) for the vID is set and biometric material is securely stored together with the vID cryptographic material in the wallet.
A 25	Functional	Authentication and enrolment might be based, not only on biometrics, but also on other traditional authentication mechanisms.	Fully	Virtual Identity issuer creates a cryptographic link inside of ARIES App so the credentials for authentication are protected by both user's smartphone and an additional chosen authentication factor (PIN or face).
A 26	Functional	After the end of the ARIES project, in case the ARIES ecosystem wanted to be released for commercialization, it should be previously tested scrupulously in a real-world scenario, with real users. (To comply with the recommendations for systems that deal with Biometric data)	Fully	eCommerce and airport use cases were piloted with real users in a controlled scenario with success.
A 27	Functional	Biometric data must be destroyed as soon as the enrolled person no longer uses the service and/or the device.	Fully	Biometric and all data from the vID are totally deleted when the user delete the vID or uninstall the ARIES app
A 28	Functional	Biometric data at rest must be always kept security protected (encrypted)	Fully	The secure wallet in the ARIES app is cryptographically protected
A 29	Functional	vID should be not transferrable, so once it is stolen it should be revoked and new independent vID must be created	Fully	The vID is linked to the handset and cannot be fully re-created. Only new one using the same electronic document may be created.
A 30	Functional	The mobile wallet might be created using specific parameters of the device, to	Fully	Architecture does not define how this should be achieved, provided implementation (via

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
		link it univocally with the device.		SDK) used device fingerprinting to ensure the link.

Table 4: Functional requirement compliance matrix

2.2.2 Non-functional requirements

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
1	Security	**Authentication:** All components of Aries must use authentication protocols to mutually authenticate. Each communication between the Aries components, between any hardware token and the Aries client and between the service provider shall only take place after a successful mutual authentication.	Fully	All backend components used TLS, selected parts provide extra security on top.
2	Security	**Data_Integrity:** All components of ARIES must protect the integrity of the eID data, metadata and logfiles during transport and at rest.	Fully	Data persisted in Secure Vault and with the required protection. Identity link was persisted in Virtual Identity Issuance server and also protected.
3	Security	**Confidentiality:** All components of ARIES must maintain the confidentiality of data during transport and at rest.	Fully	All components were using TLS.
4	Security	**Tracing:** All ARIES components should ensure that no tracing of eIDs is possible by unambiguously identifying an ID without the knowledge of secret information or by linking several eIDs of the same user.	Partially	No tracing was possible based on public data. Pilot implementation did not include privacy proxy, tracing was possible for the vID verifier (SP information).
5	Security	**Access control:** All ARIES components must enforce appropriate access rules such that only authorized persons or instances are allowed to access eID data, metadata or other security relevant data (e.g. cryptographic keys).	Fully	The architecture supports this feature, nevertheless organization and proper access management was not setup fully for the pilot.
6	Security	**Client_Standards:** The client should comply with relevant communication and interface standards, communication	Partially	The architecture is designed to support these standard protocols and were used for pilot. In case of laws the assessment was not done for the pilot.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
		protocols and laws and must correctly implement them.		
7	Security	**System_Standards**: The System should comply with relevant communication and interface standards, communication protocols and laws and must correctly implement them.	Partially	The architecture is designed to support these system standard protocols and were used for pilot. In case of laws the assessment was not done for the pilot
8	Security	**Physical:** The backend infrastructure of ARIES should run on a site that implements appropriate physical site security measures to prevent unauthorized physical access to ARIES servers and storage facilities.	Fully	The architecture supports this and ARIES backend can run on any appropriate site, but it was not fully demonstrated for the pilot.
9	Security	**Replay:** Every authentication protocol between ARIES internal components and between token and client and between service provider should be resistant against replay attacks.	Fully	Implemented solution used transient sessions with strict state machines and session expiration mechanisms.
10	Security	**Provider:** The service provider and identity provider must implement standards, protocols, cryptography, etc. used for communication with ARIES correctly and must protect their own server infrastructure against malware and unauthorized access.	N/A	Cannot be assessed for the pilot as full organization was not set up.
11	Security	**Personnel trustworthiness:** The ARIES backend infrastructure should be operated by trustworthy personnel and system administrators. The entity running the ARIES service must ensure that only trustworthy personnel obtains access to ARIES servers and data.	N/A	Cannot be assessed for the pilot as full organization was not set up.
12	Security	**Token standards:** The hardware tokens used for logon to ARIES should comply with relevant standards, cryptography requirements, authentication protocols and protection profiles (if available) and must correctly implement them.	N/A	No hardware tokens with protection profiles were used for pilot.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
13	Security	ARIES ecosystem should provide **unlikability** feature to ensure effective pseudonimity when necessary.	Fully	Fully provided by Idemix and partially by anonymous PKI implementation.
14	Security	Aries ecosystem should provide **transparency** property. It aims at clarity of all privacy-relevant properties and actions so that all stakeholders in a system are aware of and can understand its function, potential risks or consequences of own actions	Fully	Since ARIES system can provide transparency requisites to end-user, it was not implemented for the backend part of the pilot setup.
15	Security	ARIES ecosystem should provide **intervenability** to User or other parties involved. Deals with the possibility for Users or other parties involved in a system to intervene if necessary.	Fully	Since ARIES system is designed to provide all prerequisites, this requirement was not demonstrated during pilot.
16	Usability	**Effectiveness:** The user should be able to use the interface effectively. This means that the user must be able to fulfil their designated goals towards the ARIES client. All key tasks MUST be able to be fulfilled by all target user groups, having no prior training or being laypersons.	Fully	The UI of ARIES app is designed in a very intuitive manner, giving instructions in the screen and minimising the buttons and clicks to perform task
17	Usability	**Efficiency:** Users should be able to accomplish their goals related to the ARIES client quickly. Especially when it comes to repeated functionality (e.g. authorizing at a system every day), users MUST be able to fulfil their goals in what they would consider reasonable time (as e.g. can be measured by perceived ease of use). Security technologies like encryption might slow down response times significantly. Even if computation of a function takes time, the user interface of the clients SHOULD stay responsive at all times.	Fully	Once the enrolment is done (only one), the usage of the vID (repeated functionality) is performed in very reasonable time and reducing the interaction needed.
18	Usability	**Satisfaction:** The user should have a sense of satisfaction when using the system and accomplishing tasks. This	Fully	After the pilots execution, a very positive feedback from tester has been obtained on relation to satisfaction of user experience perspective.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
		implies a system that MUST provide a reasonable effort for fulfilling a certain task (i.e. simple functions should be simple to use) and MAY be fun to use.		
19	Operational	**Support of different business cases**: Different stakeholders and different scenarios require different business cases. There is no existing business case that fits all use cases. Therefore, ARIES must support different use and business cases.	Fully	eCommerce, boarding and duty-free use cases have been demonstrated during pilots. In addition, the architecture of the ARIES app provides Secure Vault inspection use case.
20	Operational	**Provide added value for all stakeholders involved:** Stakeholders are relatively satisfied with the solutions they currently use for authentication. This implies that, to implement Aries, all relevant stakeholders should be provided with some added value, e.g. additional revenue; cost savings, usability, privacy or security benefits.	Fully	The usage of ARIES app drastically reduces the authentication time (eCommerce, boarding) giving a high level of assurance benefit to the remote digital onboarding processes.
21	Operational	Support of **different deployment models**: Different stakeholders and different scenarios require different models of deployment. There is no deployment mode that fits all use cases. Therefore, ARIES must support different deployment models.	Fully	Architecture of ARIES ecosystem is designed as different pieces that can be used separately, giving ARIES the possibility to integrate easily with third party software.
22	Operational	**Interoperability:** Different scenarios, uses cases and business cases are characterized by different services and authentication methods. Therefore, a great variety of services and authentication methods must be supported	Fully	Since the architecture of ARIES allows to integrate different authentication methods, different services can be provided by ARIES.
23	Operational	**Mobile support**: The use of mobile devices is increasing in importance for both, consumer as well as professional services. However, authentication for access through mobile devices remains a challenge in many use	Fully	Face recognition and voice recognition are implemented as part of authentication methods, using the mobile device to verify the biometric data. Others, like fingerprint recognition, could be added.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
		cases. Therefore, ARIES must support authentication through mobile devices		
24	Operational	Support of **anonymous authentication:** In some use cases users have an interest in protecting their privacy and service providers don't need personal information about the users. Therefore, ARIES should provide anonymous authentication	Fully	Anonymous authentication may be provided if no attributes are requested by the Service Provider and anonymous vID may be issued if ID Proofing step is not done.
25	Operational	Support of **non-anonymous authentication**: In some use cases, users and service providers have an interest in certifying personal information about the user. Therefore, ARIES must support non-anonymous authentication allowing the Service Providers to obtain the personal data necessary for their use case.	Fully	Level of anonymity depends on attributes and policies used. In pilot pseudonyms were used for eCommerce authentication when user account was managed on Service Provider side.

Table 5: Non-functional requirements compliance matrix

2.3 *System performance and scalability*

Performance of the system may be considered from two points of view. In the initial stages of the project it is important the response times of the application are small and the application may provide comfortable user experience. As users join the system it becomes important that the system is able to process high number of concurrent transactions and is fully scalable to allow deployment in current technologies (e.g. as provided by public clouds).

Because usability and security are at the heart of the efficiency of any biometric system, Key Performance Indicators have been defined to help assess both aspects.

2.3.1 Response times

The response times are usually measured between points when there is user interaction required. It is not important if the user is able to finish authentication including password verification below 2 seconds, but what is the time the user is waiting for the response from App or server. This has direct impact on user acceptance and may be a major blocker in case the solution is perceived as slow and user uncomfortable. Typical required response time is around 2 seconds for frequently used actions and should include all steps of processing: network communication delays, server calculations and UI reaction to the result. The actions that are done only once (e.g. during enrolment) are not so sensitive to fast reaction times.

The issuance and authentication flows have some space for optimization but are minimalistic in general. If the network communication is implemented efficiently in the App then the optimization probably would not be needed. Aries project flows always contain one or two network request-response exchanges, server calculation such as credential verification and App UI reactions that are usually negligible compared to the rest.

ID Proofing step depends strongly on the speed of NFC reading of the document and reliability of MRZ reading (in case of document with MRZ) it is recommended this step is highly optimized as it is probably the longest step in the enrolment process. The optimizations may be done at the NFC level and at the level of verification scope: the implementations may read and pre-process all data in the App and send the result to the server (to limit network communication) or the reading may be from server with App only as a proxy. Both solutions have pros and cons, usual trade-off is between security, performance and flexibility. Current state of the art implementations provides reading times between 5-20 seconds and this is usually acceptable for the users (if good feedback is provided) because it is done only once.

For biometric enrolment, the typical time to process encoding and quality verification is about 100 to 300 ms. Most of the time perceived by the end-user is related to data transmission (sending the signed reference image) and getting the feedback from the server (encrypted template). This step is typically about 1 to 3 seconds.

vID credential issuance process is usually done as a single step, so the performance target should be lower, but it is expected the reaction times should be low according to state of the art systems with similar functionality.

vID verification is an action that is performed frequently, and the reaction time of 2 seconds should be considered. For most of the cryptographic schemes it should be achievable without optimization. This was proven by pilot implementation using PKI when the solution was deployed on a server with standard parameters without any cryptographic acceleration.

For biometric verification, the time to process encoding and matching is about 120 to 350 ms. One more time, most of the time perceived by the end-user is related to data transmission (sending the encrypted reference template and the live image to match with) and getting the feedback from the server. This step is typically about 1 to 3 seconds.

2.3.2 Biometric Recognition Performance

2.3.2.1 Terms & Definitions

Any Biometric System designed for identity verification (regardless of whether we are considering an identification use case or authentication use case) can be evaluated along two high level metrics called “False Acceptance Rate” and “False Rejection Rate”. These metrics reflect the ability of the system to minimize Type I and Type II errors at a given operating point. Typically, a biometric application will choose an operating point (usually some kind of setting of a parameter or set of parameters) after which one can evaluate performance.

In statistical hypothesis testing[1], a **type I error** is the rejection of a true null hypothesis[2] (also known as a "false positive" finding), while a **type II error** is the failure to reject a false null hypothesis (also known as a "false negative" finding).

In biometric technical terms, a “false positive” means that the system has mistakenly identified an impostor as an authorized user (for example let a non-authorized person board a plane because it misidentified the impostor for an authorized user). A “false negative” reflects the inability of the system to recognize an authorized user, thus identifying said authorized user as unknown – and therefore unauthorized.

[1] https://en.wikipedia.org/wiki/Statistical_hypothesis_testing

[2] https://en.wikipedia.org/wiki/Null_hypothesis

In applicative terms, a Type I Error (or False Positive) is **a security issue**, as a failure of the system to prevent unauthorized individuals to gain access. As such, it is considered with extra care and should not be dependent on user behavior (authorized or ill intentioned) and be consistent regardless of the environment conditions.

Yet, a simple figure fails to capture the complexity of interaction in a biometric system and a user, especially when it comes to an adversarial user actively trying to defeat or circumvent the system, such as in Presentation Attacks (as defined in ISO JTC/SC1 30107 Presentation Attack Detection – or PAD - standard). In this standard are also defined KPIs and error rates specific to Presentation Attack Detection. Typically, Type I and Type II errors can also be defined for the PAD subsystem and need to be taken into account in security and usability assessment, as a PAD subsystem can either fail to detect an attack (leading to an unauthorized access) or classify a genuine attempt as an attack (leading to a false rejection of an authorized user).

Presentation Attack Detection is a complex aspect of biometric technology, with a technical framework and ecosystem being built now. ISO 30107 certainly is a turning point in this ecosystem building process, but the exact methodology for evaluating Presentation Attack Detection techniques performance are still relatively new and subject to experimentation and interpretation. For these reasons, no formal evaluation of Presentation Attack Detection performance has been performed in the scope of the ARIES project. Still, as the consortium deemed it important to have an evaluation close to the operational reality, Presentation Attack Detection technology remained activated throughout testing in order to reflect operational performance.

In applicative terms, a False Rejection is a **nuisance and a frustration to end users**, in the sense that it will force the user either to re-submit to identification, or to go through an alternate process of Identity verification. As it does not represent a security threat (except in the very specific case of watchlists – not in the scope of ARIES) it is commonly considered that it is acceptable to see Type II errors being dependent on environment conditions and user behavior (such as bad lighting can influence facial recognition or users actively hiding part of their faces).

In the frame of evaluation of ARIES biometric recognition performance, it has been considered that :

- Presentation Attack Detection would not be evaluated formally in the sense of the ability of the system to detect active attempts to submit a fake biometric sample to the system (Presentation Attack)
- False Rejections related to PAD technology would be counted as “regular” False Rejections
- False Rejections related to acquisition (known as “Failure to Acquire”) would be counted as “regular” False Rejections
- Because of the specific nature of the Identity Proofing and Verification process, Failure to Enroll rate would not be evaluated, as it corresponds typically to a failure to compare the user’s face to a reference photograph (typically read from a trusted source as a passport) and so be comparable to False Rejection rate.

2.3.2.2 Target figures for ARIES

The target KPIs for ARIES have been set as follows, as indicated previously in D4.4 [5] :

KPI #	Type of indicator	Description	Target value
25	Biometrical	False Acceptance Rate (FAR)	0.1%
26	Biometrical	False Rejection Rate (FRR)	5%

The choice for these targets corresponds to industry and operational practices. Of course as FAR and FRR are dependent (and define an operating point) one cannot set one independently from the other. The lower the FAR, the higher the FRR and vice versa.

Although FAR = 0.1% could be considered a “low bar” for security, it is consistent with what can be read from the literature as to human face recognition performance (such as in

https://www.nist.gov/sites/default/files/documents/2016/12/14/facerecognitionalgorithmssurpasshumans.pdf).

These figures are derived from operational testing from different sites installed by IDEMIA – not necessarily covering the exact use cases of ARIES, but close. Of course, a lower FAR target might be set, at the expense of a much higher FRR. It is considered that above 10%, system start being deemed "unusable" or "uncomfortable" by end users.

2.3.2.3 Operational performance for ARIES

The following report is based upon live observation of a pilot project for plane boarding.

- 119 passengers went through the boarding gate
- Measured FAR was 0%
- Measured FRR was 1.5%

These figures do not take attempts where the user is actively trying to obscure parts of his/her face from the sensor into account. Both figures comply with the set targets. Note these are pure biometric performance figures and do not integrate potential communication issues and optical reading issues.

2.3.3 Scalability

The flows as defined consider there is a session for each transaction. Each verification is started at the backend, performed between the App and the frontend and finished by backend call. This means one of the strongest constraints is a session management and the architecture design does not allow any workaround. It means if the system is to be scalable session management in cluster must be deployed for each component. The session management is not a typical session with the requests coming from the same channel, so it cannot be solved easily with sticky session mechanism but should be implemented by other means that allows persistence of the session information in database, shared cache and similar. Note that this may be optimized, but only at cost of rework of the architecture and some security features.

The modularity of the solution is also a good feature for scalability: each component may scale at different velocity and the system may be optimized according to hardware needs of each calculation. Each component may be viewed as a microservice with different hardware and scalability requirements.

2.4 *Sustainability and future extensions*

The solution is defined as modular with possibility to replace any module with a module providing same functional step and required additional features. This may be considered a strong point of Aries solution. The integration process is simple and may be achieved with a simple proxy between existing solution and Aries solution as proven during voice authentication integration, when the authentication method did not have required Aries features (authentication initiated by backend) but all were implemented in the proxy service at small effort.

The flow also considers initial handshake that should allow negotiation of the flow steps based on features available in the particular App and identity which should allow concurrent usage of old App versions and new Apps with additional features.

Modularity of App design provides a good pattern for implementation of new authentication methods as well as for new implementation of Mobile Wallet when new technology is provided in the handset for protection of user data. The extensions should be simple and should impact only build of the application: the Mobile Wallet is only a dependency package that may be replaced by new version without any impact on existing code.

In the future, part of the processing required to be conducted at the moment on the server side to be trusted may be migrated back to the end-user device with new mathematical approaches like Verifiable Computation, improving both performance and privacy.

3 Legal evaluation

The information of the legal requirements in the table below is extracted from previous submitted deliverable D2.3 as they were described in the Annex. However, those related to information society services legal framework and consumer's rights have not been included since they will only apply once the exploitation of the services starts. Although D2.3 [1] Annex also contained some requirements on electronic signatures, this part of the analysis was done just if any of the ARIES tools uses digital certificates. As this has not been the case, they have not been taken into account for the purpose of this document. Therefore, the following table is only referred to the legal requirements related to e-ID and Legal Enforcement Authorities (LEA). Privacy and GDPR compliancy has been analysed in section 2.1.2 of this deliverable.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
eID1	Legal	The applicant must be aware of the terms and conditions related to the use of the electronic identification means	Fully	Consent Form and Project Objectives and procedures were provided to participants
eID2	Legal	The applicant must be aware of recommended security precautions related to the electronic identification means	Fully	As part of the procedures, instructions and recommendations are provided to better understand the security context
eID3	Legal	The applicant must collect the relevant identity data required for identity proofing and verification	Fully	In pilot implementation minimum data was obtained and erased from servers of the solution.
eID4	Legal	The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid	Fully	The ID Proofing process leveraged on existing ID Documents. Validity information was obtained from the document only. It may be further improved by using document blacklists.
eID5	Legal	It must be known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same	Fully	The ID Proofing process leveraged on existing ID Documents and the verification take into account life recognition.
eID6	Legal	One of the following alternatives has been selected: a) The person has been verified to be in possession of adequate evidence; b) An identity document is presented during a registration process; c) Except procedures have been used previously in the same Member State for a purpose other than the issuance of electronic identification	Fully	Option b was implemented.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
eID8	Legal	The electronic identification means characteristics assure that it utilises at least two authentication factors from different categories and that it is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.	Fully	In pilot possession of handset with Aries App and biometric feature were used as authentication factors.
eID9	Legal	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs	Fully	Security of delivery was assured by existence of session (protected by shared random session ID).
eID10	Legal	It must be possible to suspend and/or revoke an electronic identification means in a timely and effective manner	Partially	Revocation of Aries vID in possession was implemented. Revocation was not implemented for lost documents, but implementation options were discussed. The project did not consider any central process of revocation to minimize personal data retention.
eID11	Legal	There must exist measures taken to prevent unauthorised suspension, revocation and/or reactivation	Partially	Processes implemented for Aries vID in possession, not implemented for stolen or lost vID.
eID12	Legal	Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met	N/A	Reactivation was not implemented to minimize personal data retention on server side.
eID13	Legal	Renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level	Fully	In pilot re-issuance of vID based on the same document was implemented.
eID14	Legal	The release of person identification data must be preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication	Fully	All personal data (including identification) are protected by Mobile Wallet application and protected by password in pilot setup. In production instances other protection means may be implemented (fingerprint, face recognition).
eID15	Legal	Where person identification data is stored as part of the authentication mechanism, information is secured in order	Fully	See dataflow analysis.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
		to protect against loss and against compromise, including analysis offline		
eID16	Legal	The authentication mechanism must implement security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms	Fully	See dataflow analysis.
eID17	Legal	There must exist a published service definition that includes all applicable terms, privacy police, conditions, fees and any limitations of its usage	Fully	Term and conditions are provided in the app and in the documentation given to the participants associated to the consent form.
eID18	Legal	Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information	Fully	The different components of the architecture already consider policies to control the data management.
eID19	Legal	There must be an effective information security management system for the management and control of information security risks, that adheres to proven standards or principles for the management and control of information security risks	Partially	The pilot instantiation already provided effective measures, although a more formal risk analysis will be required on the different possible instantiation, that actually is out of scope of the project.
eID20	Legal	There must exist proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed	Partially	The architecture defined already identify different procedures to provide security properties in the whole cycle. Missing a complete risk analysis but that depend on the different possible instantiation of the architecture.
eID21	Legal	Electronic communication channels used to exchange personal or sensitive information must be protected against eavesdropping, manipulation and replay	Fully	See dataflow analysis.

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
eID22	Legal	There must be procedures to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches	Partially	See eID19.
eID23	Legal	All media containing personal, cryptographic or other sensitive information must be stored, transported and disposed of in a safe and secure manner	Fully	The usage of secure wallet and secure vault provide this functionality.
LE1	Law enforcement	There is a way to comply with LEA requests of information about the users' activity	Fully	Pilot provided example flow of audit log inspection by LEA using Secure Vault.
LE2	Law enforcement	Users will be informed about law enforcement data processing when signing up the ARIES system	Partially	The terms and conditions would have to be updated to illustrate the routing rules: i.e. data concerning the citizens of a specific member state being copied from the local vault where the identity provider is operating to the member state vault.
LE3	Law enforcement	Access must be given to the users' data stored in the Secure Vault when it is necessary for the performance of a task carried out by a LEA	Fully	The Secure vault is only accessible after LEA request and user gives consent using app.
LE4	Law enforcement	When a different Member State law enforcement agency needs to obtain information from the Secure Vault a direct access is not allowed.	Fully	This is supported through the architecture: - the vault is supporting routing of messages to a specific member state or to various of them depending on the local regulations (according to the issuer/user/hosting regulations) - the deployment architecture enables a per-member state instance - each instance has its own escrow keys for law enforcement This design allows data segregation both logically and physically
LE5	Law enforcement	There is a way to check that requests for disclosure sent by LEA are reasoned and do not concern the entirety of a filing system or lead to the interconnection of filing systems	Fully	The LEA could get access to all the data stored within the local vault. Routing rules provide the segregation on the data: they are stored in the specific vaults. Even if a LEA is looking at the complete local secure vault, only the data routed to it will be accessible.
LE6	Law enforcement	LEA are only allowed to retrieve requested information among the different transactions on READ-ONLY basis.	Fully	The escrow key provides READ-ONLY access, no write capabilities

Req. ID	Type of requirement	Description of the requirement	Compliance	Implementation
LE7	Law enforcement	All the LEA requests will be logged to keep the full history of investigation events	Fully	All LEA requests are tracked and recorded to the local secure vault, and depending on the configuration and the citizenship of the user, sent also to its country vault..
LE8	Law enforcement	The ARIES interface should inform the LEA that data obtained cannot be processed for purposes incompatible with those related to prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security	N/A	The interface is a web service, not a graphical user interface

Table 6:Legal requirements compliance matrix

4 Socio-ethical evaluation

The foundations of the ARIES approach to the social and ethical aspects of its planned activities were laid out in its deliverable D2.2 **¡Error! No se encuentra el origen de la referencia.**

This document was used as a guide throughout the project to ensure that socio-ethical aspects were included in its work. It included summaries of workshop finding, and the framework the project was to adopt to undertake ethical impact assessments. These assessments were further developed in deliverables D4.3 [4] and D4.4[5] where a "how to" audit like checklist was used across both pilot scenarios to ensure a consistent ethical approach was adopted.

The deliverable D2.2 document was a comprehensive document but in short, its aim was to keep at the forefront of the ARIES work three key questions:

- Is it legal?
- Is it ethical? (proportionality and necessary)
- Is it acceptable by citizens (trust and confidence)?

The legal checks were undertaken as outlined in the previous section and the ethical and societal acceptance was undertaken during the key stages of the project.

Citizen trust and confidence was initially tested, and a snap shot of societal perspective was obtained by way of a questionnaire undertaken in Porto which focused on eCommerce and subsequently a larger online survey using the EUs survey portal which attracted over 200 responses from across the EU.

As a result of the analysis the following table below was developed. In this deliverable as part of the evaluation a final end column on the right hand side has been added for review and comments

Ethical Principle	Definition	Stakeholder Concerns	How ARIES addresses their concerns	Evaluation and Review
Pre-cautionary principle	The principle which all other principles are linked and subordinate. The obligation to "do harm."			Principle adopted
TRUST	Trust refers to the obligation to handle data in such a way as to build and sustain public trust in the data handler's commitment to legal, secure and ethical processing.	Concerns by the public that whoever handles their data can be trusted to do so in compliance with legal principles and respect ethical practice. This includes the principle of no loss of control of data and respect for the principle of the right to be forgotten. This places high expectations and obligations on data handlers.	Aries is designed to maximise the potential for generating sustainable public trust in a reliable virtual eID that minimises the chance of fraud. That is a core goal of the project.	Trust and Confidence surveys and evaluation questionnaires have been an integral part of both the online surveys and pilot survey questionnaires. In general people felt they did trust a neutral eID and ARIES technology to preserve their privacy through the Aries virtual eID, keep their personal data safe and limited to proportionate and agreed use, and therefore would be happy to use a system going forward.
Proportionality	No data other than that which is explicitly required for the	If more data is requested than is necessary, there is the probability that insufficiently precise	The virtual eID is designed to elicit only that information that is intrinsic to the	Participants were pleased to see that only minimal information would be disclosed, and that that

	transaction envisaged should be used.	rules apply to stating what data should be sought and retained with the risk of mission and function creep.	transaction, and not to extract additional information or link it to any other information.	disclosure was under their control. The example used was age restricted purchases where the response was not their birthdate but rather confirmation that the user was over the minimum legal age to purchase it.
Dignity	Human rights to dignity, autonomy and equality, must be respected. This means that if a person is unable to supply the requested data for the transaction, an alternative means of completing the transaction should be provided discreetly.	E.g. For eIDs involving facial recognition, how best to accommodate individuals who wear face coverings, including burkas, masks or have had plastic surgery? For eIDs involving iris scanning, how best to accommodate individuals with prosthetic eyes? For fingerprints, in the event of missing fingers, or damaged finger pads making finger print capture impossible or unreliable, what alternative is envisaged to enable that person to access a particular service? How are disabled people's needs accommodated in a way that respects them and does not place them at a disadvantage eg in terms of timely access?	Biometric data is not stored. The kind of biometric held in the master repository of a public administration depends on the state in question. In principle, an Aries eID could be biometric agnostic: in practice, it may only be available to people able and willing to provide one or more particular biometrics (eg iris plus fingerprint/voice print/face). Transparency over biometric templates is essential especially given mixed private-public sector arrangements.	The Aries eiD system was tested with Android-based eIDs using various head coverings and disguises. It worked well in preventing access by would-be fake/fraudster claims to an identity. The data was only stored on the mobile device and can be fully deleted easily
Autonomy	The principle that a person has control and is able to exercise that control himself/herself without intervention.	A service should not compromise the autonomy of an individual by, for example, involving surveillance that is not essential to the transaction.	Aries eID enrolment is voluntary. No one may be forced to enrol. There must be an alternative means of accessing public services or online services (private or public) separately and independently of the Aries eID.	Industry feedback such as airport check-in or e-commerce did show that this would not replace other means to do these transactions but could be available if people wished and this could potentially save them time
Self-determination	The principle of personal choice. No one should be under duress.	A person is able to choose whether or not to provide the requested info, including a biometric, in the form demanded by the service provider without being	The choice of whether or not to enrol for an Aries eID is left to the individual person to decide.	As Above

		discriminated against should s/he be unable to do so. This is related to the principles of dignity and autonomy, and non-discrimination.		
Consent	A person should have the right and ability to consent to how their data is managed and used; an opportunity to not consent without then being deprived of the opportunity to access a requested service; and an opportunity to consent to any onward use.	A provider may not assume they can do whatever they like in future (including data mining, data analysis, splicing, re-sale, etc), or rely on function / mission creep business models that implicitly get a potential customer to tick a 'consent' box for vague or imprecise purposes.	Aries eID holders are informed in advance of how their information will be used, held and destroyed. An individual may request the destruction/erasure of their data at any time.	Standard consent forms were developed for eCommerce and eAirport, and are shown in previous deliverables. All data was anonymous and destroyed at end of the tests in the presence of the individuals involved. Test participation was voluntary and only adults participated.
Equality	Equal access to the service envisaged requires non-discrimination in terms of gender, age, capacity	A service may not be restricted to a given gender, educational or social group unless prescribed by law (eg access to age restricted goods and services)	An Aries eID should be universally available in future. For the purpose of the project, it is being trialled with able bodied people typical of online users.	Only able-bodied people participated. However, such things as extending time out on applications was achieved to assist individuals who needed more time to enrol and use their Aries eID.
Inclusion	People with disabilities or socially excluded people must be included in the service to be provided.	Ensuring service and data requirements are presented in an accessible manner; ensuring that if infirmity or disability compromises a person's ability to use the service, an appropriate alternative is available immediately.	Aries eIDs should be available to all in future.	Not tested but the Aries eID uses an open architecture modular approach to help ensure it will be available to all in future, and is therefore designed with scalability and inclusion in mind.
Non-discrimination	The precautionary principle in practice means that a service must be universally available and not restricted by gender, race, social class, ability to pay etc.	Automated sifting according to predetermined criteria, such as race, age, disability, background, intelligence, etc. is not ethical and is not part of the Aries eID.	Aries eIDs will not be restricted in future to those with a particular background or ability to pay high fees for the convenience and privacy gains the Aries eID seeks to provide.	This was not tested as such (e.g. no volunteer was asked to pay to enrol; no pre-screening took place to exclude pre-determined ages or races). It is not anticipated that ARIES will allow such restrictions
Purpose specification	The purpose for data handling must be presented clearly and precisely.	Vague descriptions which implicitly allow for function and mission creep are not acceptable.	Aries eID enrolment procedures make clear how data will be handled, in line with EU regulations and directives; and how onward splicing or re-	Full information about data and full compliance with EU regulations and directives will be embedded into the ARIES solution.

			use is prohibited. The virtual eID is designed precisely to enable technical measures to minimise data disclosure and linkage to what is absolutely essential for the envisaged transaction.	
Purpose minimization	The data collected or referred to must be the minimum necessary for the purpose of the service to be delivered	A vague general purpose description is unacceptable. No more data than is essential and necessary for the transaction envisaged may be collected. E.g. if a person wishes to buy age-restricted alcohol, the vendor need know only that a person is over the prescribed age. The date of birth, home address, name etc of the person are superfluous. Excessive data may not be collected and re-used.	Aries eID does not depend on a vast amount of data being accessed by the service provider, collected and interrogated. The purpose of the Aries eID is to limit data exposure so that only that which is essential for the transaction is authenticated	Minimal data disclosure can be achieved and several different ARIES virtual eID personas can be created to allow for this depending on context and setting. (e.g. for buying age restricted goods; for travel documents; for general grocery shopping etc)
Accountability	Data handlers must be accountable legally in respect of their handling practices.	An individual must have the right of redress in the event of poor handling, theft or loss. The liability of the data handler is established and disclosed to the data subject, along with information on access to redress and error correction.	The Aries project team is accountable for how data is handled and used, again in conformity with EU legislation and relevant national laws.	GDPR and project management ensured compliance
Transparency	Data handling practice must be open, clear and explicit.	How data is handled must be made explicit and understandable to the public. Lengthy T&Cs and small print are unacceptable.	The Aries eID does not assume that an enroller implicitly gives consent. Rather, explicit consent and data handling practice, in line with best practice, will be made available in future.	Consent is explicit
Privacy	Data handling must comply with the highest legal standards (eg EU GDPR). In different contexts (eg health versus online shopping for tee shorts) ethical rules and linkability issues arise that are	Data handling can be automated and/or undertaken with human intervention. There must be awareness of underlying service goals and algorithm bias. Staff accessing data must be trained in privacy	Aries does not regard privacy as a commodity only available to those who can afford to buy the highest levels of privacy security. Instead, privacy is intrinsic to the Aries eID and the Aries eID seeks	A full Privacy Impact assessment and privacy by design principals were adopted by the project. They were informed by the ethical impact assessment tool developed during the project.

	context specific. Aries recognises that.	maximising practice to ensure the privacy requirements are met. Privacy enhancing technologies alone are an adjunct not a substitute for this requirement and for privacy impact assessments. Some data are sensitive (health for example) and should be interrogated only for the purpose for which they were provided, and not therefore made accessible to insurance companies seeking business (except under the explicit and informed, autonomous consent of the individual involved). This is especially important in respect of the collection and use of biometric data from which other issues may be inferred.	to enhance privacy by technical and handling protocols to limit information exposure. This is essential to help combat attempts at accessing a service fraudulently or for unintended purposes (such as to commit a crime).	
Security	Data handling procedures must be robust to ensure that personal data are secure	Service providers must comply with the law; they must ensure their own systems are secure and robust against intrusion to prevent data loss, theft or compromise.	Aries expects the highest robust data handling practices to be practised; and accordingly recommends buy-in at the highest level of the organisation in terms of PIA and EIA.	High level industrial standards for data security were utilised. Attention was drawn to PIA and EIA compliance
Accessibility	Online services must be accessible and presented in accessible formats to all of society.	eIDs might contribute to the digital divide, whereby the wealthy and privileged have broader access to the service or can buy higher levels of privacy (that would be unethical). Accessibility means that online information must be accessible (legible or vocalised), and that those unable to see, hear of speak have alternative means of accessing the service without their dignity and autonomy being compromised	In future, accessing Aries eID online for disadvantaged users would be addressed by designers of the Aries eID public-facing portal. This would ensure respect for and realise dignity and autonomy of all.	This was not tested but the current Aries eID system is designed in manner to be adaptable and inclusive, and scalable in future

Table 7:Ethical principles compliance matrix

5 Pilot evaluation results

In order to achieve the proposed goals of ARIES, the consortium has performed three deployments of the ARIES technology to integrate, validate and analyze the results from the other WPs and receive useful feedback in two end-user driven demonstrators.

The first demonstrator aims to test the ARIES technology on the online authentication and proofing, identity derivation, in the scope of an eCommerce scenario. This has been presented and deeply explained in D4.3 [4] The second demonstrator focuses on strengthen the security, trust and privacy in identity-related processes in the scope of airport businesses, being boarding process and duty-free shopping the chosen scenarios. This second deployment was presented in D4.4[5] .

Following the schedule, the first demonstrator (eCommerce) was performed meanwhile development phase was not finished yet, providing information to WP3 to improve the developed technology with regards to usability, privacy compliance and performance. After analysed those results, second generation of the ARIES system was produced and released to be tested in the second demonstrator (airport).

5.1 *Architecture vs. pilot implementation*

Pilot solution was implemented according to the architecture defined in D3.1 but was simplified because of time constraints. In all the cases the end user experience was the same, but following features were not implemented.

- Privacy proxy in eCommerce authentication was not implemented. This feature was intended to provide privacy in front of the web Aries vID verifier to conceal Service Provider usage in case a pseudonymous identity is returned (not applicable for Idemix). This is achievable by standard means and standard protocols (SAML, Open ID Connect) and we considered it has no impact on pilot evaluations.
- Idemix implementation was done as a separate App triggered by *Intent.* The architecture always considered usage of a single App with a Mobile Wallet as security storage. The implementation did not use any Mobile Wallet as the 3rd party Idemix library did not allow this. We provided a smooth user experience as both Apps used the same look and feel.
- In the boarding use case, the airline integration was also triggered by *Intent*. As many different airlines application could theoretically be integrated with ARIES app, it will not be possible to merge both into each airline app. Nevertheless, the user experience could be improved by less dense QR Codes. But to do so, it would require to using smaller biometric templates, data format and signature to fit into a standard boarding pass QR Code.

5.2 *Voice authentication evaluation*

Voice authentication was implemented at the final stages of the project and, therefore, evaluation was not included in the deliverable D4.3. The voice authentication integration was requested by SONAE. After the necessary alignment and plan, effort was put in place to allow for this option in the ARIES system. This was most important because of the following factors:

1. The feedback from the end-user in the demonstrators, mentioned the interest of additional biometrics options so that the user can use the one that is either more convenient or just of their preference.
2. This new type of biometrics could allow in the future to enrol and use services, namely in e-Commerce, in new contexts where users can't use their hands. Let's imagine doing your groceries shopping in the car commute; or calling into the call centre and identifying yourself just by saying your name.
3. The project partners did not have any solution for voice authentication, so it was a good chance to understand the easiness of integrating with a third-party service provider opening their API for the project.
4. Finally, the project initial KPI's do mention the objective of having a multi-biometrical option for the end-users to choose from.

In summary the setup was much similar to the e-Commerce Face recognition (see D4.3 [4]), but instead of having a face recognition option, there were two with the second being the Voice enrolment.

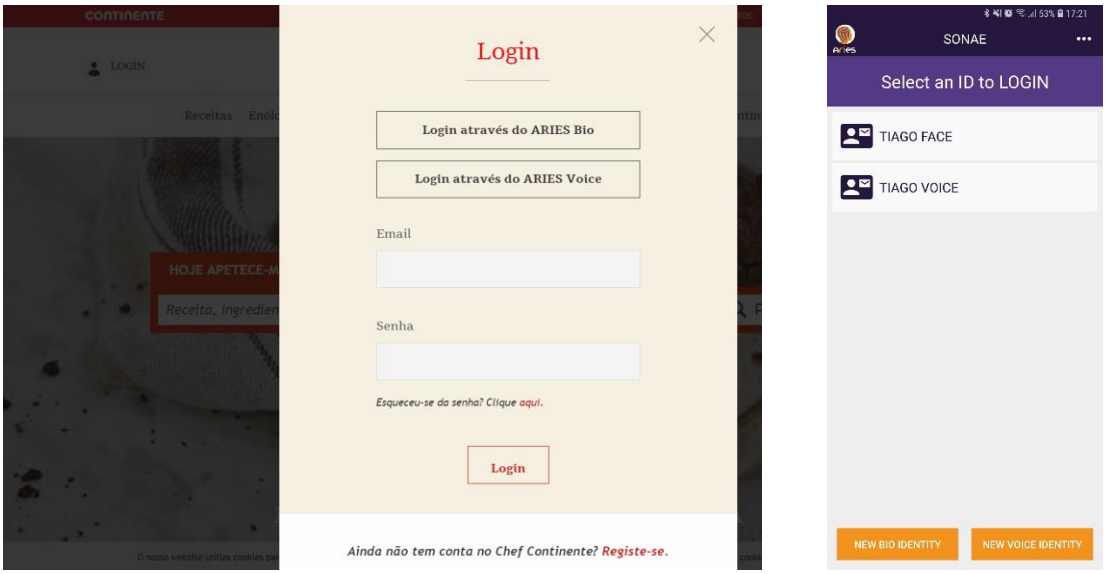

Figure 4 - ARIES Chef Online page with the Voice and Face options and app screen.

In practical terms the user uses the same app but has the option to select previously recorded ID's or just create a new ID with the Voice biometrics. If the user chooses this option, the voice will be collected and afterwards when using the Chef Online page the user can login by using their voice. The voice recognition software is based on third-party API that was kindly open for this project. The assurance rate is around 99,9%.

The Voice demonstration directly answers the users need and want for another biometric option. Other previously mentioned needs identified by the project that we selected include, Assurance, Accessibility, and Easiness of Use. The following table identifies how the Voice Recognition option works towards them.

Attribute	**Importance**	**Impact**
Assurance	High	The assurance rate of the voice recognition is over 99,9% so that system allows for a great option here.
Accessibility	Medium	The accessibility can somewhat be increased as the users can use their voice and extend the use to other contexts where the use of hands or visibility of the face is not convenient.
Easiness of Use	Very High	The easiness of the voice recognition, if higher, than the voice, the option can be very good on this attribute.

For the purpose of validation of the Voice Recognition option (but also to again validate the face option), Sonae organized a Hands On Workshop on February 8th, 2019 where members of the Advisory Board, Associated Partners, stakeholders and external users were invited to know better the project and to test the technology to give feedback on the solution.

Some of the positive feedback that can be extracted from the round table after the experimentation phase in the workshop can be summarized as follows:

- The ARIES 'App' is considered to be a useful tool, being easy to use with positive comments being received on the concept of holding duplicate electronic means of proving identity.
- The App provided citizens with a greater feeling of control and ownership of their personal identification as they are in charge of the information which will serve to tackle false and forged passports and reduce identity theft leading to cyber fraud.

- The flow of the enrolment process was positively received. The users of the App were pleased that they simply enrolled once and that this process could include self-claimed attributes such as email and addresses linking the citizen, but only to be provided if the user wanted to.
- The fact that the face recognition and voice identification capabilities would be activated for use while login in webpage as a secured identity proofing was very welcome.

5.3 *Usability*

Law enforcement agencies in the UK are committed to citizen focused neighborhood policing, delivering services and making decisions as close to communities as possible with the focus on keeping communities safe and feeling safer.

We aim to ensure that all our frontline services which include response and investigation are working together cohesively to serve their neighborhoods better. By closer joining up of the services we provide, we create a resilience in visible policing and continue to improve public confidence.

Technical solutions like the ARIES App and its features create robust secure cyber experiences that help in keeping citizen's identity safe online. The additional security features the ARIES App provides such as facial recognition as a login and high levels of encryption to personnel data increases the security layering effect. This means that cyber criminals have to overcome more factors to obtain a person's credentials and create a duplicate identity.

These along with the philosophy of not revealing a person's full credentials in situations where the person wants to prove their eligibility helps keep citizens credentials safe and ultimately communities of citizens feeling safer.

These main factors hit nine out of ten of the advice given by LEA's to citizens to help prevent them becoming a victim of crime. They are known as the ten principles of crime prevention and can be found listed and explained in D4.4[5] identity virtualization prototype demonstrator.

Law enforcement agencies would be reluctant to single out and recommend any commercial provider to citizens. They would always look to provide guidance on what features users should look for in products. The guidance helps the person establish the best products that match their needs and gives them a baseline measurement for comparative purposes.

ARIES contains many features that would be part of that guidance or recommended components that could help secure their identity and prevent them from becoming a victim of crime.

Below is the feedback from Jet2.com and Leeds Bradford Airline that indicates from a commercial and security perspective there could be an increase in public safety and customer experience by introducing an ARIES concept to the airline industry.

Enhancing the boarding processes at an airport would increase the speed of boarding, reduce the staff requirements and confirm the eligibility that the true passengers were boarding the correct aircraft at the correct gate on the verified date and time allocated. This cross referencing would increase the customer experience reduce human error factors and leave airline and airport staff with more opportunities to enhance the customer service and increase security.

Multiple users on one handset is a step forward from many ID documents which contain children or dependent details. These are currently difficult to securely reconcile with face to face verification as often there is no biometric information.

High levels of security are required at national infrastructure sites. A concept which follows the philosophy's and methodology outlined in the ARIES research project could increase the security and reduce risk of incidents that effect the sites and the regional and national economies.

5.4 *Improvement points*

5.4.1 eCommerce improvement points

Users from all the sections of the user testing, stated that the app was in good shape, that it fits the purpose of being the interface of the ARIES system. Particular notes on the good points were the general look and feel of the application, which surprised some users due to its final product-like appearance. Also, although it is a complicated workflow there were mixed opinions amongst participants about being easy to use. People noticed if it was not for the demonstration and use the app for the first time it would be a little more difficult to use. To resolve these issues positive suggestions were made to support the enrolment process with a simple video or with on-screen graphical guidelines (GIF)to help users in the process.

It was found that the demonstrations worked well, but occasionally there were impacts of external issues such as poor light and background noise that affected correspondently the face and voice recognition.

In eCommerce usability needs, such as being able to do the whole process in one device (instead of also using a laptop) and allowing for multiple device account (such as phones & tablets) is very important for consumers and the need for such is important (even over “extreme” security).

The following system improvements were identified and can be a good clue for the future of the system and its potential evolution into a product and market adoption:

1. It should be able to work on other mobile platforms (e.g. iOS) as not only Android is widely used and trusted.
2. It should use the fingerprint scanner capability of the device for the onboarding on the vID or to protect the users profile to be used instead of a password for user convenience.
3. To develop the facial recognition capability of the App enrolment and identification verification process, users suggested that the background lighting of the App needed to be improved.
4. If you have a digital passport, it could be on the cloud and restore the documents in every device - we should not need to re-login in every device we have, we should be able to import the documents to the user devices
5. With increasing levels of security and the sharing of personal data, the issue of the appropriate levels of assurance arose. ARIES app could manage level of assurance depending on the target user/service provider of the solution. If ARIES will be used for simple login, it is not necessary to use an official document derivation.

5.4.2 Airport scenario improvement points

The ARIES App was developed and tested as a proto type and not a commercially market ready product. The low number of participants that were part of the user testing means that feedback was limited during the project.

Also within the project scope there were no plans or opportunities for any independent testing to take place.

Independent testing performed by a third party would be a benefit and improve the confidence in ARIES and its philosophy and methodology. This reference point would give LEA’s and citizens another factor in which to make an informed decision on what is the best product for them. This should show how robust and secure their personal information was while being held on a mobile device and presented in a format that is easy to understand.

The information held on the server should also be independently risk assessed, to assess what information would be lost should a data breach happen and what risk that poses to the user. This should also be part of the user information.

The ARIES data vault on different devices should be penetration tested, to grade or assure users that their personal data is safe from hackers and fraudsters on whatever device they choose to buy.

The ARIES App allows multiple users on one device and it should carefully consider the way passwords are configured and administrate by the user. The use of long passwords and special characters for passwords should be encouraged and made available.

Users should be encouraged to use a secure password manager and ARIES should include a password strength indicator, consider including a password attempts rule, to lock the ARIES app for a period of time after a number of attempts.

A larger more citizen focused testing stage should be considered, where a large volume of users tests the ARIES app. ARIES should be tested using forms of identification from different countries and different breeder documents.

In the feedback from Jet2.com and Leeds Bradford Airline they highlight some improvements that they would need before ARIES could be considered and asset they would deploy. They highlighted that a concept like ARIES would need to account for the very complex issues surrounding international Visa's and their management by airlines and airports, they would also require confirmation by an airline or airport agent that a passenger is in possession of the paper travel document (passport, ID card) for when they arrive at their destination, passengers can be refused entry at the destination and this is a cost met by the airline company.

More robust testing to verify that using facial recognition and a barcode reader does in fact speed up and streamline the boarding process. The potential benefits of speeding up the boarding process would allow more time for passengers to shop in the departure lounge which generates revenue for the terminal.

With specific reference to the boarding use case, users described that passengers are often concerned about the boarding time but do not realize the queue is due to security checks. They went on to state that sometimes citizens lose the security perspective as users. Positive aspects revealed that as a third-country national has to be physically registered in front of a border police officer, if authorities were allowed to use ARIES for means of identification, they could use ARIES at the enrollment level of trust for that specific purpose. Furthermore, when Schengen systems will be in place, ARIES could be used because border police will have all the system parts at the same level of security and trust, meaning it could be used in a non-infrastructure border location making it a desirable system

6 Conclusions

ARIES project has a goal to provide reliable framework for electronic identities derived from electronic document and using biometric authentication. The goal was approached in several steps: generic architecture definition, implementation of selected version of components for end-user pilots and implementation of proof of concept components to show the solution is not limited in terms of cryptographic scheme or biometric feature used.

In order to verify project results requirements were defined for several domains: ethical, legal and technical and also GDPR compliancy was also set as mandatory requirement. The project was evaluated with following findings:

- Requirements were fulfilled at architecture level, yet few requirements require organizational setup and other measures. Architecture on its own provides a guidelines, real security and privacy depends on each implementation.
- Pilot implementation covered the requirements with expected open points regarding application deployment, supporting infrastructure and organization. Goal of the pilot was to provide a proof of concept and a real end-user experience, not a fully setup solution ready for production.
- The evaluation was supported by two additional proof of concept service deployments: Idemix (zero knowledge proof technology) and voice authentication to demonstrate the solution is flexible and extensible.

The pilots performed with several groups of end-users provided a valuable feedback on user experience and transparency of the solution. The project pilot implementation was more advanced than expected by the audience yet it was obvious that in order to start production many open points need to be solved.

- iOS support
- More extensive user tests with emphasis on feedback, help and guidance through the process
- More implementations of Mobile Wallet should be provided for user that would like to use fingerprint of face ID authentications
- ID recovery procedure should be provided
- More streamlined integration path for airline companies to issue boarding passes should be provided
- Boarding terminal should be optimized for faster QR code reading

7 References

[1] Deliverable D2.3 "*Legal requirements and analysis of ID legislation and law enforcement aspects*" ARIES project, 2017

[2] Deliverable D2.1 "*Analysis of Identity procedures, life cycles and their weaknesses*" ARIES project, 2017. Classified document.

[3] Deliverable D2.2 "*Socio-ethical analysis and requirements*" ARIES project, 2017

[4] Deliverable D4.3 "*Secure eCommerce prototype demonstrator*" ARIES project, 2018

[5] Deliverable D4.4 "*Identity virtualization prototype demonstrator*" ARIES project, 2018