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

ARIES

"reliAble euRopean Identity EcoSystem"

D2.4 – Privacy and data protection compliance report

Due date of deliverable: 31/08/2018
Actual submission date: 31/08/2018

Grant agreement number: 700085
Start date of project: 1 September 2016
Revision 1.0

Lead contractor: Atos Spain sae (Atos)
Duration: 30 months

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	

D2.4 – Privacy and data protection compliance report

Editors
Julián Valero and Mar Antón (UMU)

Contributors
Julián Valero and Ignacio Alamillo (UMU)
Juliet Lodge and Dave Fortune (Saher)

Reviewers
Melissa Wild (POCC)
Juliet Lodge and Dave Fortune (Saher)

31-08-2018
Revision 1.0

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

Document History

Version	Date	Author(s)	Description/Comments
0.1	23/07/2018	Julián Valero and Mar Antón (UMU)	Determination of privacy legal requirements
0.2	25/07/2018	Juliet Lodge and Dave Fortune (Saher)	Addition of privacy ethical requirements
0.3	04/08/2018	Julián Valero, Ignacio Alamillo and Mar Antón (UMU)	Privacy risk assessment and analysis
1.0	31/08/2018	UMU and Saher (with comments by GTO, ATOS and POCC)	Final version

1 Executive Summary

As GDPR came into force on 25th May 2018, the use of personal data in ARIES needs to meet its requirements. The aim of GDPR is to ensure that user's data is respected and organisations adhere to the rights and freedoms of users. The objective of this report is to analyse how the diverse components of ARIES ecosystem treats personal data, its compliance to GDPR requirements, as well as providing recommendations to mitigate risk. The report also includes an ethical assessment, which provides the context for the further legal analysis.

It has been prepared considering the content and requirements of Data Protection Privacy Impact Assessments (DPIA) within GDPR legal requirements, and other related documents produced by data protection authorities and standardization initiatives. As set out by *Article 29 Data Protection Working Party*, in the process of building and demonstrating compliance with personal data protection regulation, a DPIA has an essential role to play. Using this tool as data controller, ARIES has to "describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them"[1]. From these premises:

- This report includes a systematic description of the data processing by ARIES.
- Necessity and proportionality are assessed considering their legal foundations.
- Risks to the rights and freedoms of data subjects are identified, assessed and, therefore, managed according to the Article 35 GDPR requirements.
- Finally, not only the severity and likelihood of the risks are estimated but also the adequate measures envisaged to treat those risks are determined as well with the aim of eliminating, reducing or accepting them in a proportionate level.

The structure of the report has been adjusted to the referred requirements. After the initial ethical assessment (Section 3) the content of DPIA under GDPR is explained (Section 4), ending with the legal assessment of the risks and threats to which personal data is subject within ARIES ecosystem (Section 5). The results of this analysis have been confronted with a standardized methodology through PILAR application, offered by the Spanish Government (Section 6). Therefore, risks has been analyzed in various dimensions (confidentiality, integrity, availability, authenticity and accountability), including the residual risk along all the data treatment phases. Finally, this report contains a series of recommendations with a list of measures to be adopted with the aim of mitigating the risks that an ARIES solution may present when being commercially exploited.

[1] *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, page 4.

Contents

2 Introduction

2.1 *Purpose of the document*

The main objective of this document is to offer the required guidelines to ensure that the outcomes of the project comply with applicable data protection laws and principles, in order to facilitate their future practical usability according to Regulation (EU) 2016/679. From a privacy perspective, the nature of ARIES project demands the application of a specific evaluation with regard to both use cases: E-commerce and Airport scenarios. This evaluation aims at making technical and organizational decisions that minimize sensitive data exposure and it will be carried through a Data Protection Impact Assessment of the proposed system. It is also informed by the Ethical Impact Assessment prepared for the project.

2.2 *Relation to other project work*

Although the report refers to the whole ARIES ecosystem, it is clear it has a close connection with Section 5 of D2.3 *Legal requirements and analysis of ID legislation and law enforcement aspects*. The DPIA is also based on the analysis of the data processing described in Section 2.2 and 3 of D3.2 *Virtual identity developments.* This deliverable is connected as well with privacy by design guidelines (MS 5 in WP2) and system architecture (WP3).

2.3 *Glossary adopted in this document*

For a better understanding of the deliverable, it is convenient to underline that for its preparation the following legal concepts have been used according to the GDPR definitions:

- *biometric data*: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- *consent*: a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- *data controller*: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- *personal data*: any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- *processing*: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- *processor*: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- *profiling*: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- *pseudonymisation*: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- *recipient*: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- *third party*: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

3 The data protection impact assessment (DPIA) in Regulation (EU) 2016/679.

Under Regulation (EU) 2016/679, all data controllers and processors are obliged to apply data protection methodologies by design and by default (art. 25 GDPR). This necessarily implies the application of several complementary and successive methodologies:

▪ Analysis of the risks involved in the processing. This aims to identify risks not only for data security but for the rights and freedoms of individuals as well.

▪ Identification of the measures necessary for the processing to:

- eliminate or mitigate risks;
- be developed under the requirements of privacy by design in order to:
  - ensure data quality,
  - limit the volume and categories of data necessary for the purposes of the processing,
  - and adopt functional and appropriate safety measures for the processing.

The privacy impact assessment is an obligation under Regulation (EU) 2016/679. The aim of the rule is to improve compliance with the Regulation in cases "where processing operations are likely to result in a high risk to the rights and freedoms of natural person", as Recital 84 GDPR states. In this context, there are mandatory requirements setting out when a data protection impact assessment should be developed. Article 35 provides for the deployment of such assessments in some cases

> *where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*

Even if it is not strictly imposed by law according to the above-referred provision, ARIES assumes a set of measures, including the DPIA, which includes a framework for guaranteeing the rights of the persons concerned, as expressed in the project Grant Agreement that must:

> *consider evaluation of the minimum data sets required for electronic identities and derived identities, evaluation of the use of electronic and derived identities, based on the principle of data minimization, identification of logical separation mechanisms between the primary identities and the derived identities and assessment of re-identification mechanisms applicable to dishonest use of derived identities*

This deliverable is intended to meet the objectives set out in article 35 GDPR:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this

Regulation considering the rights and legitimate interests of data subjects and other persons concerned.

4 The data protection impact assessment in ARIES ecosystem from an ethical perspective

The ARIES ecosystem is designed with privacy and ethics in mind. The dominant ethical principle to be observed in practice is that of 'do no harm' known as the pre-cautionary principle.

Accordingly, when preparing the tests, the ARIES test projects asked the same set of questions and adopted the same methodological approach to ensure consistency across all of the ARIES activities:

- Fitness-for-purpose. How is ethical use designed into the system?
- What biometric(s) is used and why?
- Have algorithms been interrogated for bias?
- What are the risks and benefits of the solution envisaged to users?
- How can any risks be mitigated? Is it safe to proceed? What are the implications for technical development of the solution? What are the implications for users?
- What adaptations may be necessary for the user? Can they be achieved?
- What are the risks and benefits to the business model of adapting technical solutions in the light of the tests? Would those identified adaptations be more user friendly?
- How have ethics been designed into the technical solution envisaged? Is this sufficient from the point of view of user trust building?
- Privacy by design supports but is not a substitute for ethics tests, an EIA and stringent ethical compliance. The above questions were refined as appropriate, informed by a common methodology and set of assumptions.

As a reminder, guidelines and rationale have been expanded in Deliverable.2.2.

4.1 *The inherent risk of doing inadvertent harm*

From an ethical perspective, any data enrolment, collection or (manual or automated) processing must not harm the data subject directly or indirectly. It must be proportional to the purpose for which processing occurs, must minimise data used and ensure that it is used for that one, specific and limited purpose only. That means it must be minimised. No more data should be enrolled or collected and associated than is expressly necessary for the transaction envisaged. It must not be open to re-purposing, reconfiguration, onward selling and use, notably without the explicit informed consent of the data subject. Any site that relies on ticking the box on terms and conditions to infer consent is acting unethically and not in the spirit of the GDPR. Breaching the spirit of privacy preservation under the GDPR is a breach of ethical practice.

ARIES is aware that in the general context of an eCommerce scenario, what matters is disclosure of the means to pay the amount for the intended purchase; any age restrictions on purchasing (e.g. alcohol); and – where delivery of ordered items is required – a delivery address. All other information is superfluous to the transaction. Privacy and ethical practice are observed if this is practised. If it is not, and more information is required and enrolled and disclosed to the service provider (in the above

instance, home address, date of birth, marital status, number and ages of children, possession of pets, types of insurance) privacy and ethical practice are not observed sufficiently. As non-observance may be very tempting for a service provider —and not all of the above-referred data are required for the ARIES purpose— neither payment nor delivery information have been included in the eCommerce demonstrator. However, ARIES recognises that in real world transactions such information may be collected for legitimate purposes, as well as for purposes where the same information would be disproportionate or excessive to the completion of the transaction.

4.2 *The risk of discrimination – escalated risk owing to biometrics*

Any e-service that relies on a user being wealthy enough to buy a device to enrol for it, is discriminatory and fails the justice and equality tests. ARIES, relies on smart phone user tests, and in that sense may be theoretically discriminatory.

Any personal data that has to be collected in order for a person to access the service envisaged (eCommerce; eAirport) may not be collected in a way that discriminates against vulnerable users (disabled, children, injured) and therefore this means that the service must be available to those users through an alternative means of enrolment and authentication. Inadvertent harm may be done to a person if they cannot access the service on the same conditions as, for example, able-bodied users; if the system discriminates against them enrolling in and using it; if they have to provide more information than the prospective e-user.

Biometric information is especially sensitive. The ethical and legal requirements governing its use are diverse and complex, and sometimes contradictory. ARIES should be aware that even though the use of biometric data may be legal and meet legal requirements, it might be disproportionate to use biometrics in the use intended. Biometrics may also present risks to the integrity and autonomy of the person – especially if such data is either LINKED to, or LINKABLE with, other data. Such as if the data is poorly administered; badly stored; spliced, re-used or used for a purpose for which it was not originally collected (in the case of eAirport, and ecommerce, it may allow re-interpretation and analysis to discriminate by age, ethnicity, gender).

ARIES is acutely aware that the definition of what constitutes a biometric varies significantly across states. Increasingly, the US definition that included all behavioural data that could be collected and associated with a person/data subject or item, raised specific ethical and privacy objections in the EU that were associated with intelligence gathering, monitoring, surveillance by private and public (state) bodies inside the state or outside it. Such information gathering and specifically linkage is seen as disproportionate to the objective for which is may be collected for eCommerce purposes. Anyway, although ARIES has been designed to be biometrics agnostics if the service provider (the service using ARIES) does not require biometrics, face recognition in the eCommerce use case is included just to demonstrate the technology. Where eAirport use is concerned, particular problems arise in that fly-and-shop data may be useful to agencies combating crime, to intelligence and border agencies. Their use of such data is usually covered by exceptions regulated by legal provisions.

ARIES notes that therefore any onward use of information associated with a biometric (face, fingerprint, gait, hand print, vein print, ear print, voice print) infringes ethical principles as well as privacy requirements. Purpose limitation and purpose specification are taken very seriously and technical steps have to be built-in to prevent onward use.

ARIES is aware that it is completely unethical for minors and the vulnerable to be targeted or persuaded to use eCommerce without appropriate, strong safeguards being in place to safeguard their privacy, autonomy and integrity. The ARIES EIA indicates points at which these can be checked.

4.3 *Onward use and linkage risks – business models and convenience*

Onward use risks in eCommerce relate to: access by other agencies (banks, finance companies, credit risk and credit checking agencies, advertisers, trackers and their associated companies inside and outside the EU). Such access may be a business case for commercial opportunities but the practice is unethical potentially. It also presents privacy intrusive risks and therefore would not meet GDPR requirements. This means that the customer using eCommerce, that there is a conflict between the convenience gained of eCommerce and the potential for tracking and intrusion by other companies. For example, a person ordering chocolate cake online may receive emails or 'offers' relating to baking, investing in cocoa, cosmetics, clothes, trips to the zoo and travel as a result of the company providing the good having sister or parent companies operating in various other fields).

eAirports and the use of eID credentials present challenges from the ethical perspective. ARIES acknowledges the interest of crime combating agencies to frustrate fraud and international organised crime, including impersonation, something that biometric data are designed to hinder.

ARIES trials the eID in eAirport in full awareness that the potential to link that data with other data (often intelligence defined behavioural tracked data) adds value and interest to that data for purposes of combating crime.

Consequently, from the legal and ethical perspective, eID eAirport must specify precisely the conditions under which such data may be made available in part or in full to other, legitimate *state* agencies for a precise, clear and specific purpose defined by them. ARIES is also aware that governments do outsource action to combat crime to private companies whose staff enrolment and training practices may not meet the ARIES ethical and privacy requirements.

Under ARIES eAirport, the working assumption is that high quality and rigorous technical and administrative processes and standards are in place. However, onward data use or re-use and linkage cannot be wholly prevented by the eAirport ARIES eID without making onward linkage under any circumstances technically impossible.

4.4 *Risks to integrity, equality, dignity, justice and autonomy – Real time, real person scenarios*

ARIES virtual identity is tested with users using mobile devices. ARIES recognises that the reliance on mobile devices immediately poses ethical issues relating to:

Autonomy, dignity, equality, discrimination, justice, inclusion and the pre-cautionary principle.

Evaluating the ARIES solution with users using mobile devices goes beyond recognising the potentially discriminatory implications of reliance on a device that may be too expensive for users to acquire or that may pose accessibility problems (or gains) for disabled or infirm potential users. Therefore, in further development, Aries ID service providers would have to offer alternative accessible and convenient means to enroll/ use service.

At each step ARIES examines whether the authentication possibilities opened by the ARIES approach make the use of an eID via a smart device more accessible to disabled users who might otherwise be disadvantaged by the technological device on which the ARIES virtual eID relies.

Test: validation of chosen biometric, such as light dependence for quality images, dampness of fingerprint, dry or colour of eyes, gait, ability of user to use iris, voice, facial recognition ports (eg many cannot keep still long enough; speak defects or dysarthria; tremor; dementia; age; visual defects; physical disabilities) etc.

Ethical risks to the autonomy and integrity of a person arise notably from the linking in part or full of data collected for one purpose but used or associated in part of full with other data that will have been collected for a different purpose, at a different time, possibly months or years apart, in a different place. Such data may have different rates of degrading, obsolescence and error. The reliability is therefore compromised.

Accountability for reliability raises legal and ethical requirements, liabilities and consequences. This applies even if the linkage or partial or full association has been done automatically. The ethical implications are far-reaching in terms of the potential harm that may result for a live citizen using the eID enabled service: a genuine eID created by a genuine person (using his own biometrics) but deriving an identity from a stolen or genuine unused blank official identity document allows him to commit further crimes, to the detriment of the legitimate owner of the identity. Any information derived from tracking that and associated with the legitimate owner can harm his credit ratings (and therefore ability to access all manner of services), his general history and cause him significant economic, reputational harm, inconvenience and lengthy harm in re-establishing his entitlement to that identity. Without that identity intact, the traces of breach and intrusion may follow him forever, thereby compounding the original harm both to the citizen himself and to the company with whom harm is associated.

How ethical is it to deny a legitimate person such access? ARIES adds ethical value in providing for a way to allow him to re-establish and use his identity by virtue of the ARIES validated eID.

ARIES credentials collected for one purpose but linked to another – occasionally countries may impose temporary bans on people with certain medical conditions from entering their country. If an eID or biometric (such as dna) allows access to all manner of information files on a person's medical history, contacts, social and educational background, it would be unethical and contrary to legal requirements to allow that.

Nevertheless, this is a risk and possible.

Consequently, ARIES is aware that restricting the agencies that may have access/ or see (without having a right to download, copy, link and amend) still requires that their personnel have mutual recognition of access rights and criteria in place. That would conform with ethical standards and practice. But as it is a longer term goal, ARIES proceeds on the basis that no access beyond the silo of the organisation responsible for eCommerce and eAirport is technically feasible.

4.5 *Information gap risks*

There is a significant information gap where the public's knowledge of ethical and privacy obligations on the part of service providers is concerned.

The understanding of good practice in data handling of eID data was evaluated during the trials. Participants were asked explicitly about how they would like best practice to be communicated more generally in order to boost public awareness of:-

- Personal responsibility for sufficient and essential good data handling and management practice (eg keeping personal data safe; and, for those who are disadvantaged (mentally or physically) how they can do so)
- Awareness of the obligation on data handlers providing services to honour ethical principles, especially data and purpose specification, minimisation, dignity , consent and compliance with the law.
- Methods of making information about this readily accessible and understandable.

ARIES, throughout the project, has made particular efforts to inform voluntary participants of what the ethical codes and privacy requirements are; and how their data will be used and destroyed.

The ethical and legal requirements for enrolling and authenticating biometric data must be made clear. A biometric is not essential to a transaction: it may be a convenience gain in terms of speed of transaction to the service provider, and the citizen. It may be a precondition of using eAirports. But in most other applications, the biometric is not essential. Citizens are unaware of this.

It is equally doubtful that the citizen using eIDs for any purpose, is sufficiently aware of the consequences of enrolling one or more biometrics; and how this can be associated to other data and linked/spliced, re-used for more generalised tracking and privacy intrusive purposes by unseen others. This is especially problematic in the case of epayments using biometric enrolment for ecommerce in schools with minors paying by fingerprint, for example.

It is vital to define precisely the limited purpose for which an eID algorithm has been created; and to be open about issues around how inter-operability and portability promise convenience gains to citizens IF certain conditions are met. Insufficiently resilient eIDs, and those not informed by the principles of ethics by design risk allowing greater scope for intrusion and manipulation (mission creep, info-seep). Information linkage has commercial advantages. It is key to security intelligence. At one level, this may be desirable (eg linkage of info for public sector service delivery, maximizing Big Data and Open data potential). At another level, it is risky and potentially harmful.

Automated decision making (bots, AI, 'smart' interaction) could deny a person a necessary service or puts them at risk of physical harm (non-entry through a smart border gate, inaccessible bank account, or a smart self-driving car being unable to decide whether to swerve or hit a person or animal). The GDPR may cover automated decision making but does not cover the potential harms consequent upon actual physical harm. Instead, developers have looked to issues about liability, and liability insurance. Both are necessary but insufficient. Built-in ethics by design may eventually deal with this, just as PETs, de-identification protocols, quantum proof encryption and privacy by design are to improve cyber security and boost smart resilience against cyber-attacks.

The cost and complexity of monitoring compliance makes more vital the development of a trustable, dependable technical ecosystem to guarantee privacy, build and sustain sufficient trust.

It is doubtful that automated enrolment and authentication adequately meet privacy and ethical tests.

In terms of realising the goals and aspirations of the Digital Single Market, eCommerce and eAirport are important steps.

A big risk scenario arises in the case of inter-operability within and across borders. DNOS happens and without alternative means of accessing the service, harm occurs to the potential user. Incompatible and legacy systems across providers and borders may deny a legitimate user, access to a service (such as banking, eCommerce etc). Liability for any harm has to be defined. Citizens must be informed of responsibility, accountability and liability paths and redress. Redress may not be discriminatory – that is, depend on the ability to pay for it.

For using eIDs outside the project, ARIES partners would be expected to observe the highest standards and comply with the EIA and PIA recommendations of the project. Reputational damage, as well as economic damage arising from poor service and or litigation, to companies can occur if EIAs and PIAs are not observed therefore observance is part of the business case developed.

5 The data protection impact assessment (DPIA) in ARIES ecosystem

5.1 *Structure and general approach*

The legal analysis of the DPIA has been deployed in six phases:

I. Questionnaire on data processing activities
Submission of a questionnaire to partners. In addition, evidence will be required during the implementation phase that can be verified under the DPIA. The questionnaire required:

- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;
- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- (f) where possible, the envisaged time limits for erasure of the different categories of data;
- (g) where possible, a general description of the technical and organisational security measures referred to in article 32(1).

II. Description and analysis of data processing activities carried out by each partner in order to identify how information flows and to describe their scope

III. Identification of the general privacy safeguarding requirements from the perspective of GDPR for ARIES ecosystem

IV. Identification of privacy risks arising from the personal data processing carried out by each of the partners, particularly:

- (a) unauthorized access to personal data by third parties;
- (b) wrongful modification/deletion of data;
- (b) excessive collection of data;
- (c) inadequate linkage of data from different processing activities;
- (d) collection of personal data without the consent of the user and problems related to its documentation;
- (e) lack of transparency from the user's perspective, including problems related to previous information and the exercise of their rights;
- (f) excessive period for the retention of personal data.

V. Privacy risk analysis and evaluation in order to determine the most appropriate measures to tackle all the privacy risks. According to Recital 76 GDPR "the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk".

For this purpose, we have applied a scale of values that relates the probability of materialization of a vulnerability to the severity of the impact on processing:

Likelihood	
Description	Level
Very likely	4
Relevant	3
Limited	2
Unlikely	1

Level of impact	
Description	Level
Very severe	4
Relevant	3
Limited	2
Irrelevant	1

This is the scale provided by the Spanish Data Protection Agency, but we could use another one (i.e. ISO/IEC 29134:2017)

VI. Proposal of privacy risk treatment options in order to elaborate privacy risk treatment plans bearing in mind the principles of RGPD, particularly:

- (a) use of anonymized data when it is not incompatible with the purpose of processing;
- (b) implementation of security safety measures as an additional guarantee;
- (c) ensuring the application of data protection by the design and by default, in the design and use of all ARIES tools;
- (d) ensuring that security measures and other legal requirements not only are implemented but can be verified as well.

5.2 *Brief description of personal data treatment in the ARIES ecosystem*

As stated above, Article 35.7 GDPR establishes the obligation that the PIA includes, at least, a systematic and detailed description of the treatment, analysing its necessity and proportionality. Likewise, it is indispensable to make a clear description of the elements which intervene in each phase of the data lifecycle, since it is essential for the adequate assessment of the privacy risks. The aim of this section is to comply with that requirement by explaining both general aspects of ARIES functioning, which imply the treatment of personal data, and those particular characteristics presented by the use cases.

Therefore, general information about ARIES from the perspective of personal data legal requirements is provided below, particularly according to the functional description of data processing and its lifecycle:

- Identify and describe the origin of personal data, their utility for the project, how does ARIES get them and who supplies the information. We should also determine the legal foundation

for each data processing (articles 6 and 9 RGPD) and proportionality requirements, particularly for biometric data, according to article 37.5 RGPD.

- Storage of personal data, where they are being stored, if back-up copies are made, recovery systems...
- Who (or what tool) can access the data, for what purpose and what kind of treatment is allowed for each subject (only access, modification, deletion, printout, download...)

5.2.1 General aspects

The details of data flows are presented in ARIES D3.2 (Section 2.2), it explains both general data flows and where they occur in the use cases (e-commerce and airport scenarios). Moreover, the adopted design and implementation decisions regarding the demands of the privacy by design principle (Section 3) are specified in the mentioned D2.3.

However, considering that Deliverable 2.3 on Virtual Identity Developments is a confidential report, for a greater clarity in the identification and management of privacy risks it becomes essential, at least, to offer a brief summary of the treatment operations within ARIES ecosystem. There are two differentiate phases – Registration and Authentication– during which the following data flows can be identified:

I. Registration

- *Initialization*: no personal data are collected.
- *ID Proofing*: once the required data are verified, they are signed and encrypted by the service and sent back to the client, according to what demands the minimisation principle set out in Article 5.1.c) GDPR.
- *Biometric enrolment*: private biometric information needed for the future authentication is collected. Nevertheless, they are not stored at rest in server-side during the enrolment process since, once processed on the server, they are signed, encrypted and sent back to the mobile for storage. During the biometric authentication all the data are used during the authentication and discarded afterwards.
- *vID issuance*: this service creates the credentials including user attributes and sends the credentials to the user. The information is not persisted in the vID Issuance service and the audit log persisted in Secure Vault should contain only pseudonymous reference of the newly created credentials (ARIES ID).

During this phase, audit log information is stored in the in the Secure Vault: document reference, biometric reference and vID reference.

II. Authentication

- *vID authentication*: the information to be shared depends on user consent and, therefore, if the sharing is rejected then the information is not submitted even to the vID Verifier. After the information is submitted to the Service Provider the user loses control over it.
- *Biometric authentication*: performs live acquisition of the biometric feature and comparison with the previously prepared information from the biometric enrolment. All the data are used during the authentication and discarded afterwards.

During this phase, audit log information is stored in the Secure Vault: ARIES ID and authentication metadata.

5.2.2 Use cases

5.2.2.1 E-commerce scenario

In this scenario customers employ ARIES digital mobile identities for both registration and authentication at the E-commerce online site. Firstly, users must enrol in ARIES ecosystem that provides them with a digital identity. Afterwards, when a user attempts to buy products in the E-commerce website, ARIES will perform user's authentication and, if necessary, a live biometric authentication against biometric service as well, using mobile device sensors (i.e. camera to capture user's face).

In the registration process, the users can link their real physical identity with the ARIES vID through a breeder document in order to increase level of assurance of the identity. The user proves his real identity through biometrics, matching the live capture of his biometrics with the ones stored in the breeder document. During authentication, users are met with stronger mechanisms as an additional authentication factor (biometry) is accomplished, and the user has full control over his information.

5.2.2.2 Airport scenario

This process will involve LEA officers at the airport in case the breeder document has been lost or stolen. Passengers will interact with airport services using a virtual identity to prove certain attributes for enabling access to the services. The IdP encompasses different services such as the Identity proofing service to validate that the user is the genuine person, the biometric enrolment service, as well as the virtual Identity Issuance in charge of generating the virtual IDs. The Service Provider provides the service that users want to get access to and it could be:

- Access Control Point at the boarding gate. Users not only have to demonstrate their real identity but also a valid boarding pass as well. The authentication takes places at the airline desk using a boarding terminal system, endowed with a camera and a screen. The user shares the biometric token stored in the smartphone obtained during enrolment to the biometric verifier service deployed in the boarding terminal. It obtains a live capture of user's biometrics to perform the biometric comparison with the biometrics used in the enrolment and only if comparison is affirmative the passenger is authorized to go onto the plane.
- *Airport Shop* in order to confirm that the user has a valid boarding pass during shopping within an Airport terminal. The shop assistant can check the age of the passenger if necessary depending on the product (i.e. alcohol, tobacco).

5.3 *Basis and legal principles applicable to personal data treatment in ARIES ecosystem*

5.3.1 Basis

Treatment of personal data by ARIES is based on the consent of users, according to Article 6.1.a) GDPR. Likewise, with respect to biometric data Article 9.2.a) GDPR also applies and requires this consent to be explicit. Nevertheless, that consent is not necessary and does not provide a legal ground for processing personal data by Law Enforcement Authorities (LEA). The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require ARIES to comply with any request of information that respect the legal requirements. This obligation is not subjected to article 6.1.e) GDPR but to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

5.3.2 Minimisation and proportionality

It is fairly clear from the description stated that the purpose of the treatment of personal data of ARIES ecosystem users consist of facilitating users' identification to third parties, called service providers, who solely must access to the information that is absolutely essential for their activity. Consequently, following the minimisation principle, knowing users' identity will be sometimes by no means necessary. The same happens in commercial activities examples, when in order to purchase some products evidence of being of legal age would be enough information.

From the proportionality perspective, it is needed to evaluate if the aim pursued with the data use can be achieved by other means that may imply a lower risk, particularly when biometric data are involved[2]. As the European Data Protection Supervisor (EDPS) has stressed, biometric data reduces the likelihood of successfully forging a document and, consequently, it may be considered as a legitimate anti-fraud measure. However, the processing of biometric data constitutes a limitation on fundamental rights, which implies that is prohibited in principle and there are a limited number of conditions under which such processing is lawful; even more, given the particularly sensitive nature of biometrics data, it will be necessary to provide for appropriate safeguards[3].

Following the guidelines of the Spanish Data Protection Agency[4], there is a necessity to analyse each treatment in accordance with the requirements proportionality, which implies three successive assessments:

- suitability criteria: if the measure can achieve the proposed objective;
- necessity criteria: if, additionally, it is necessary, meaning that there is no other more moderate measure to meet this goal with the same effectiveness, particularly when using biometric data;
- proportionality criteria in strict sense: if the measure is balanced, because there are more benefits for the general interest than damages for other assets or values in conflict. However, the definition of the 'general interest' may be subjective, or based on a commercial or political strategy. Therefore, stritcly speaking, proportionality criteria requires the treatment to be in

[2] Working Party Article 29: *Opinion 3/2012 on developments in biometric technologies*, pages 7-9.

[3] *Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents*, pages 8-9

[4] *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*, page 20.

line with the goal sought and, consequently, if it can be achieved without the envisaged measure, it has to be considered disproportionate.

Regarding this premise, in the e-commerce case, the user's identification is not essential for the service provider, except when the purchase requires the user is of legal age. The same happens in the airport scenario when it comes to buying goods at duty free shops since further information is not required. By contrast, verification of passengers' identity becomes essential when boarding a plane. In this last case, using biometric data can be crucial.

That said, regarding that the users' activity can be unlawful, it is necessary to ensure that the LEA have access to the transaction logs stored in the secure vault in case of identity fraud, misuse, liability or cybercrime investigation, as stated in D 2.3 (Section 5.2). In these cases, access to information cannot lead to a profiling activity generally, but it has to exist a direct relation between the profile creation and a concrete investigation that is being conducted. As access to personal data by public authorities affects to this fundamental right, consequently its scope should be interpreted restrictively. In that case, this is a proportionate step required for security which may, already, allow greater access under security exception laws.

Apart from other detailed requirements in D2.3, it has to be noted that the European Court of Justice has clearly stated that access of public authorities on a generalised basis to the content of electronic communications affects the very essence of the right to privacy. Therefore, the ARIES provider is only obliged to reveal users' data to LEA in the context of a concrete inquiry. As Recital 21 of Law Enforcement Directive clearly demands, "the requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems".

On the other hand, the use of biometric data demands not only users' consent under Article 9 GDPR – which has to be explicit– but also a more rigorous application of minimisation and proportionality principles, limiting the access to those cases and actors that inevitably need to use them to achieve their goals and there is no other alternative.

In the case of online and mobile services it is likely that there will be data transit between image acquisition and the remaining processing stages. Therefore, "the data controller must take appropriate steps to ensure the security of data transit. This may include encrypted communication channels or encrypting the acquired image itself. Where possible, and especially in the case of authentication/verification, local processing should be favoured"[5]. Even more if we take into consideration that facial recognition still is an immature technology[6].

5.4 *Legal evaluation of ARIES ecosystem risks*

To not disregard any of the risks, the legal analysis will be conducted following the various operations for the processing of personal data described in Section 4.2 of this document. The assessment must be performed according with the parameters set on the table of Section 4.1 thereof.

5.4.1 Registration

- Lack of information on the conditions of Article 7 GDPR about when consent if properly given

[5] *Opinion 2/2012 Article 29 Data Protection Working Party on facial recognition in online and mobile services*, page 9.

[6] Spanish Data Protection Agency: *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, page 35.

    - Although it is unlikely to happen given ARIES ecosystem (1), this is a very severe risk (4), as it could invalidate data processing. However, ARIES website/app privacy police should include a comprehensive and detailed explanation.
- Lack of information on the rights recognized by Articles 12-22 GDPR
    - Although it is unlikely to happen given ARIES ecosystem (1), this is a risk with limited impact (2), as those rights are recognized regardless of whether users are informed or not. However, as additional measure, this information should be available on ARIES website as well.
- Lack of documentation which demonstrates the consent for the processing has been given, overall in respect of the related to biometric data, which needs to be explicit
    - This is a very severe risk (4) as it could invalidate the information treatment, although it is unlikely (1) to happen because ARIES ecosystem has considered it.
- Regarding ID Proofing phase, the possibility to either access or preserve data excessively:
    - is an unlikely risk (1), since ARIES ecosystem is designed to apply the adequate security measures to avoid this happens; anyway users have the burden of preserving their data properly and preventing unauthorized access to their own terminal. However, regarding the technology employed, the risk could rise to relevant level (3), overall because of the data's nature.
- In relation to the Biometric enrolment phase, the possibility of accessing and preserving data excessively:
    - is an unlikely risk (1), as ARIES does not preserve data after its processing. Moreover, it adapts to other security measures during communications. However, regarding the nature of the information, the impact may be very severe (4), as it affects biometric data which could facilitate identity theft.
- During vID issuance phase, there is a risk that a third party has access to the credentials while carrying out their issuing. This is unlikely (1) to happen due to the implementation of the proper security measures, although the impact could be relevant (3), as it would allow an improper user of virtual identity by a third party.

5.4.2 Authentication

- During *vID authentication*, there is a risk that users reveal excessive information related to their attributes.
    - Although is the user who has the final decision about the information to be submitted and the use of the service, the ARIES verifier has included an option to filter the information for the service provider that may be seen as a last fault safe.
    - In any case, concerning access to information while communications between ARIES and user take place, the risk can be described as unlikely (1), form ARIES perspective, as appropriate security measures have been adopted in order to avoid it.
- Also, when *vID authentication* happens, there is a limited risk that the system does not work temporarily (2). In this case, the impact will be determined by the possibility of using the service. The consequential damages are presumed to be not too significant as they will last only for the interruption period (2).
- In relation with *biometric authentication*, there is a risk that the service provider requires its use against the demands of proportionality and minimization principles:

  - Although is the user who has the final decision about the information to be submitted and the use of the service, the ARIES verifier has included an option to filter the information for the service provider that may be seen as a last fault safe.
  - In respect of unauthorised access, despite the risk is limited (2), security measures are adopted since the potential impact can be high (4) as long as sensitive user's information could be caught.
  - A point to consider include potential coercions to force the use of the biometric authentication system with a very severe impact (4), but the truth is that the risk is unlikely (1) to happen. This is either because there is no enough incentive to do so (E-commerce use case) or the scenario where it would take place is public (boarding case) and it is usually monitored by a third party.
- Concerning the information stored in the Secure Vault, there are various identified risks that present an important impact (3), as ARIES allows to gather user's information in a centralized manner which could lead to reveal some aspects of user's privacy or those that affect his fundamental rights:
  - Despite there is certain risk that the information preserved is excessive, the truth is that ARIES design reduces it (1) following principles of minimization, proportionality and pseudonymisation. This way, it only preserves absolutely necessary data (document reference, biometric reference and vID reference). However, a very severe risk (4) potentially exists as very sensitive information may be affected.
  - Preserving information in excess. ARIES does not allow gathering biometric information and there is only a reference that is stored, in a way that the risk is limited (2).
  - Access to the information by unauthorized third parties, beyond LEA's use for the exercise of its functions and ARIES for the provision of its service whenever it is required. This would be a relevant risk (3), as it can lead the user to suffer discrimination both in the labour environment and general aspects of social life, since this risk could have an impact on the user's reputation whenever some habits or the consumption of certain products are revealed.
  - Access to excessive information by unauthorized third parties, due to either the quantity of information or the lack of legitimacy for accessing when justified requirements are not met. Here, although the risk is limited by ARIES design (1), security measures must be applied to prevent the access to be general depending on the relevant impact (3) that it would have. Under this situation, controls must be established case by case, in order to verify the legality of each access.
  - Use of information for different purposes by the subjects legitimate for the processing, either by ARIES or LEA. Even though the risk is limited (1) by ARIES design, it could cause problems of diverse nature, such as:
    i. In the first case, user's profiles could be created from which try to obtain an economic profit by means of either personalized advertising or the sale of personal data. Here, impact would be limited (2) as this risk is not considered as a serious damage for the affected party except in the event that the information is given to unauthorized third parties with no consent.
    ii. In the second case, there is a risk that the information is processed unfairly either in legal proceedings or investigations. In this point, the risk of affecting fundamental rights is potentially higher (3), since it could lead to imposition of

penalties and even interfere in the defence of fundamental rights due to unlawful processing of personal information.

- Undue treatment of information or, even, thereof to be deleted affecting this way to public interest to prosecute illegal activities. Although the risk is unlikely (1) thank to ARIES security measures, the level of impact is only limited (2) since there are always other ways of investigating which would allow to obtain fair proofs.
- Preserving information during an excessive period time. In this case, the risk consists of the possibility of processing data improperly, infringing demands of legal protection, which is a difficult problem to be addressed (3) as it is not easy to fix a uniform period of conservation for all EU Member States. The impact would be limited (2) as the unlawfulness of the proofs based on this data could be argued.

5.4.3 Other questions of general scope

Apart from users' register and identification processing, two general assumptions affecting the well-functioning of ARIES ecosystem as a whole could be added:

- Inability to demonstrate the compliance of processing activities with the GDPR obligations. In this case, it might not be a risk for users as it is about pure formal matters (1), except that it implies the inability to provide the service and therefore it would be necessary to obtain their consent again. Thereby, the impact could be irrelevant for users (1), not beyond that little inconveniences, while, in contrary, for ARIES could imply a penalty.
- Lack of a mechanism for the exercise of user's rights under GDPR and the proper attention thereof within the fixed period of time. In this case, there is a risk that those rights are infringed (4), although impact would be limited (2) as users could complain to the corresponding control authority on data protection for its safeguard. Here, damages would be of moral character as, in other case, preventing measures could be adopted by that authority.

6 Information security risk analysis

The ARIES ecosystem has been created considering privacy needs and thus the components allow the deployment of solutions that comply with the Privacy by Design principles.

But as any other solution based in information technology, an ARIES-based solution is subject to risks that affect different security dimensions, including:

- [A] Availability
- [I] Integrity
- [C] Confidentiality
- [Auth] Authenticity of users and information
- [Acc] Accountability of service and data
- [PD] Personal data

In the following section we introduce the value model of the assets considered in the risk analysis. The value model is needed to define the criticality of the assets and, thus, decide which security measures are needed.

6.1 *Value model*

6.1.1 Assets considered in the risk analysis

Layer: [B] ARIES Processes

The ARIES Processes are defined as essential assets, because they embody the technical components of a concrete instantiation in a solution scenario:

[IdP_UserEnrol] ARIES user enrolment process
[IdP_UserAuth] ARIES user authentication process
[IdP_UserBioAuth] ARIES user authentication process with biometrics

Each process is valuated in terms of each information security requirements (availability, integrity, confidentiality, authenticity of users and information and accountability of service and data).

Layer: [IS] Information services

The ARIES Processes are implemented using different information services. Thus, we can say that processes depend on information services. This is why the valuation of the processes will be accumulated upon the information services.

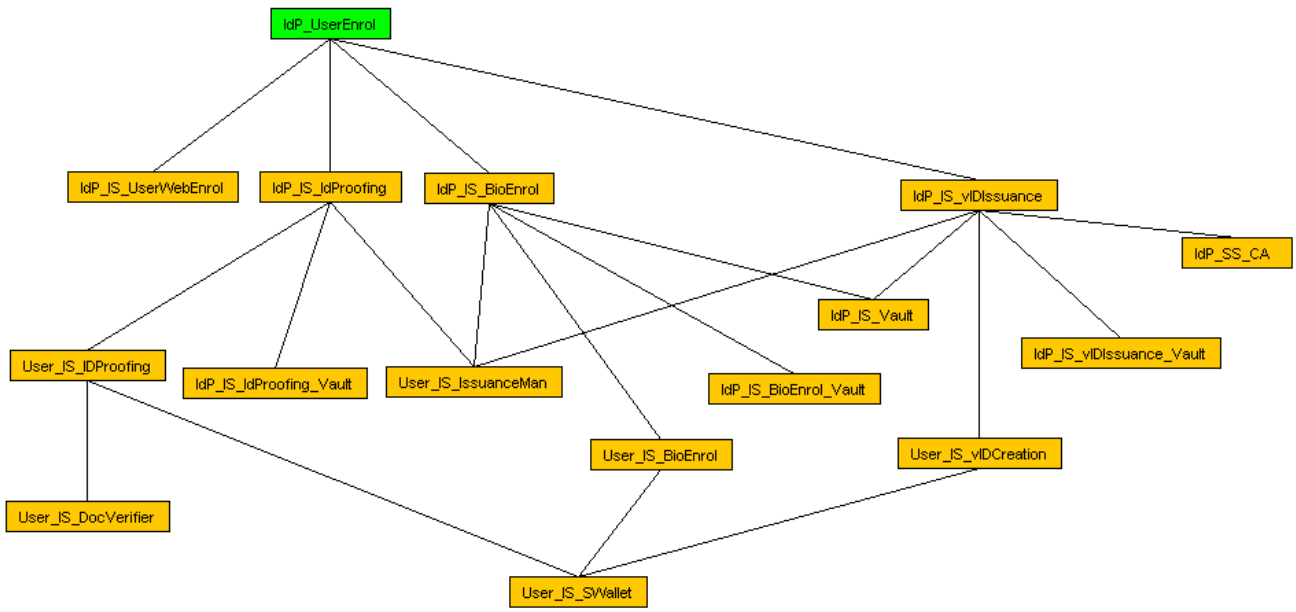
[IdP_IS] ARIES identity provider's IS
[IdP_IS_UserWebEnrol] Enrolment web application
[IdP_IS_IdProofing] ID proofing service
[IdP_IS_IdProofing_Vault] ID proofing service individual service vault
[IdP_IS_BioEnrol] Biometric enrolment service
[IdP_IS_BioEnrol_Vault] Biometric enrolment service individual service vault
[IdP_IS_Vault] ARIES secure vault service

[IdP_IS_vIDIssuance] Virtual identity issuance
[IdP_IS_vIDIssuance_Vault] Virtual identity issuance individual service vault
[IdP_IS_vIDVerifier] vID verifier service
[IdP_IS_BioVerifier] Biometric verifier service
[User_IS] ARIES user's IS
[User_IS_IDProofing] ID proofing client
[User_IS_DocVerifier] Breeder document verifier
[User_IS_BioEnrol] Biometric enrolment client
[User_IS_vIDCreation] vID creation client
[User_IS_IssuanceMan] Issuance manager
[User_IS_SWallet] Secure mobile wallet
[User_IS_IdSelector] Identity selector
[User_IS_BioAuthN] Biometric AuthN client
[User_IS_vIDAuthN] vID AuthN client

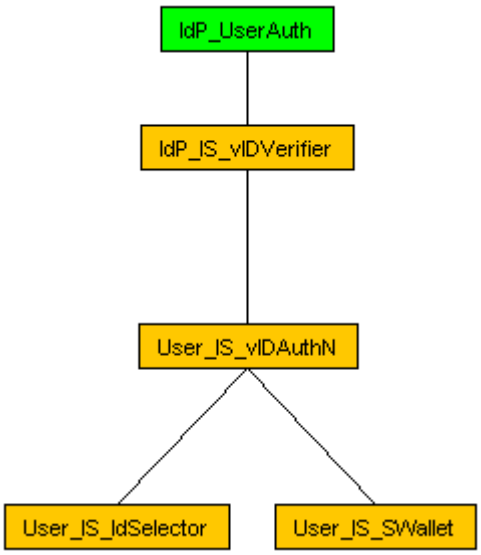
6.1.2 Asset dependencies

In this section we show the aforementioned dependencies in a graphical way, for each process.

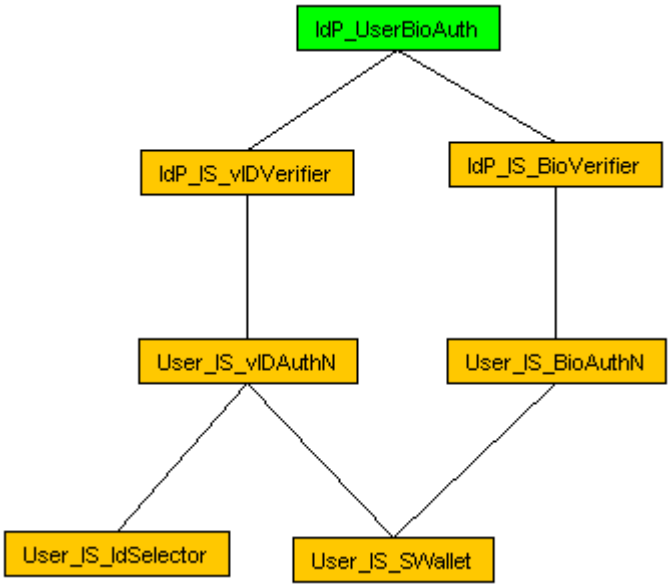
ARIES User enrolment process



ARIES User authentication process



ARIES User authentication process with biometrics



6.1.3 Valuation of assets, per domain

In this section we show the global valuation of the assets, per security domain. The valuation consists of a table with one first column that list the valuated asset, and six colums – [A] Availability, [I] Integrity, [C] Confidentiality, [Auth] Authenticity of users and information, [Acc] Accountability of service and data and [PD] Personal data – containing the asset value for the corresponding security dimension, using a number between 0 and 9.

0 means that the asset has not a value, while 9 means the maximum value of the asset. Some assets have not an own valuation, but receive it via dependencies. In this case, the corresponding box is empty.

Each valuation has an upper number related to the criteria used to set the value. The criteria are listed below each table.

RTO means Recovery Time Objective and it is used in the Availability security dimension.

layer: [B] ARIES Processes

asset	[A]	[I]	[C]	[Auth]	[Acc]	[PD]
[IdP_UserEnrol] ARIES user enrolment process	[4](1)	[4](2)	[7](3)	[5](4)	[5](5)	[5](6)
[IdP_UserAuth] ARIES user authentication process	[7](7)	[4](2)	[4](2)	[4](2)	[4](2)	[3](8)
[IdP_UserBioAuth] ARIES user authentication process with biometrics	[7](9)	[4](2)	[5](4)	[6](10)	[6](10)	[5](11)

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

layer: [IS] Information services

asset	[A]	[I]	[C]	[Auth]	[Acc]	[PD]
[IdP_IS_UserWebEnrol] Enrolment web application						[1](1)

[IdP_IS_IdProofing] ID proofing service						[1](1)
[IdP_IS_BioEnrol] Biometric enrolment service						[4](2)
[IdP_IS_Vault] ARIES secure vault service						[7](3)
[IdP_IS_vIDIssuance] Virtual identity issuance						[1](4)
[IdP_IS_vIDVerifier] vID verifier service						[1](4)
[IdP_IS_BioVerifier] Biometric verifier service						[4](5)
[User_IS_SWallet] Secure mobile wallet						[7](3)

(1) [1] Limited: Interested parties may find non-significant inconveniences.

(2) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(5) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4 Assets valuation, per asset

In this section we show the specific valuation of each asset, including the attributes used to describe the class of asset, the security domain to which the asset is related, a description of the asset, the source that documents the information about the asset, the assets on which this one depends on, and the value itself.

The valuation consists of a table with one first column that list the valuated asset, and six colums – [A] Availability, [I] Integrity, [C] Confidentiality, [Auth] Authenticity of users and information, [Acc] Accountability of service and data and [PD] Personal data – containing the asset value for the corresponding security dimension, using a number between 0 and 9.

0 means that the asset has not a value, while 9 means the maximum value of the asset. Some assets have not an own valuation, but receive it via dependencies. In this case, the corresponding box is empty.

Each valuation has an upper number related to the criteria used to set the value. The criteria are listed below each table.

RTO means Recovery Time Objective and it is used in the Availability security dimension.

6.1.4.1 [IdP_UserEnrol] ARIES user enrolment process

- [essential] Essential assets
- [essential.info] information
- [D.per] personal data
- [D.per.normal] normal personal data

- [D.per.normal.1] identification data (name and surname, id, postal address, email address, telephone, ...)
- [D.per.normal.2] personal characteristics (civil status, date and place of birth, age, sex, nationality, ...)
- [D.per.regular] regular personal data
- [D.per.sensitive] sensitive personal data (art. 9)
- [D.per.sensitive.11] biometric data
- [essential.service] service

Security domain

- [base] Identity Provider

Description

[D3.1] This process enables users to obtain a new ARIES virtual ID in the ARIES ecosystem, provided they firstly proof their identity through a breeder document or another eIDAS authentication mechanism,

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Below (assets on which this one depends on)

- [IdP_IS_UserWebEnrol] Enrolment web application
- [IdP_IS_IdProofing] ID proofing service
- [IdP_IS_BioEnrol] Biometric enrolment service
- [IdP_IS_vIDIssuance] Virtual identity issuance

Value

dimension	value	accumulated values
[A] Availability	[4](1)	[4]
[I] Integrity	[4](2)	[4]
[C] Confidentiality	[7](3)	[7]
[Auth] Authenticity of users and information	[5](4)	[5]
[Acc] Accountability of service and data	[5](5)	[5]
[PD] Personal data	[5](6)	[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

6.1.4.2 [IdP_UserAuth] ARIES user authentication process

- [essential] Essential assets
- [essential.info] information
- [D.per] personal data
- [D.per.normal] normal personal data
- [D.per.regular] regular personal data
- [D.per.pseudonymous] pseudonymous data (art. 4, 6, 25, 32, 40, 89)
- [essential.service] service

Security domain

- [base] Identity Provider

Description

[D3.1] This process allows authenticating a prior enrolled user by employing his issued virtual identity, whence requested by a service provider. This vID verification process does not imply biometric authentication. This stage also includes the privacy-preserving partial virtual identity proving, to demonstrate the SP certain attributes, complying with the minimal disclosure principle.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Below (assets on which this one depends on)

- [IdP_IS_vIDVerifier] vID verifier service

Value

dimension	value	accumulated values
[A] Availability	[7](7)	[7]
[I] Integrity	[4](2)	[4]
[C] Confidentiality	[4](2)	[4]
[Auth] Authenticity of users and information	[4](2)	[4]
[Acc] Accountability of service and data	[4](2)	[4]

[PD] Personal data	[3][(8)]	[3]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

6.1.4.3 [IdP_UserBioAuth] ARIES user authentication process with biometrics

- [essential] Essential assets
- [essential.info] information
- [D.per] personal data
- [D.per.normal] normal personal data
- [D.per.regular] regular personal data
- [D.per.sensitive] sensitive personal data (art. 9)
- [D.per.sensitive.11] biometric data
- [essential.service] service

Security domain

- [base] Identity Provider

Description

[D3.1] This process allows authenticating a prior enrolled user by employing his issued virtual identity, whence requested by a service provider. This vID verification process implies biometric authentication in scenarios that require higher levels of assurance. This stage also includes the privacy-preserving partial virtual identity proving, to demonstrate the SP certain attributes, complying with the minimal disclosure principle.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Below (assets on which this one depends on)

- [IdP_IS_vIDVerifier] vID verifier service
- [IdP_IS_BioVerifier] Biometric verifier service

Value

dimension	value	accumulated values
[A] Availability	[7](9)	[7]
[I] Integrity	[4](2)	[4]
[C] Confidentiality	[5](4)	[5]
[Auth] Authenticity of users and information	[6](10)	[6]
[Acc] Accountability of service and data	[6](10)	[6]
[PD] Personal data	[5](11)	[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

6.1.4.4 [IdP_IS_UserWebEnrol] Enrolment web application

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.www] world wide web
- [SW] Software

- [SW.std] standard (off the shelf)
- [SW.std.www] presentation server
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.1] Web portal providing a user-friendly interface for the ARIES enrolment process. It allows user to scan a QR code with its smartphone in order to trigger the enrolment process.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [IdP_UserEnrol] ARIES user enrolment process

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[4]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data	[1](12)	[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual [7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

6.1.4.5 [IdP_IS_IdProofing] ID proofing service

- [D] Data / Information
- [D.e-files] encrypted data files
- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.1] This service has the primary objectives of validating that the user owns a recognized identity. It authenticates the users, remotely checking the validity of its credentials by means of the authentication with the chip included in the breeder document e.g. ePassport, or eID. The service also checks the consistency between the face picture stored in the chip and a fresh capture of the face image of the user.

[D3.2] The ID Proofing starts with an anonymous request from the App to the ID Proofing service. The service collects following private information: - Data read from the electronic document (face image, age, name, document id). The full scope of the reading depends on policy of the reading. - Face image from live capture.

All the data are processed on server-side for trust reasons: - Checking data signature through passport Public Key Directory - Checking data signature through the public key of the issuing authority of the eID document - Checking live face capture against the reference portrait extracted from the electronic document

Once the data are verified, they are signed and encrypted by the service and sent back to the client. There is no data persistence in server-side, besides audit log information stored in Secure Vault with very limited scope (document id).

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design
- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [IdP_UserEnrol] ARIES user enrolment process

Below (assets on which this one depends on)

- [IdP_IS_IdProofing_Vault] ID proofing service individual service vault
- [User_IS_IDProofing] ID proofing client
- [User_IS_IssuanceMan] Issuance manager

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data	[1](12)	[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual [7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

6.1.4.6 [IdP_IS_IdProofing_Vault] ID proofing service individual service vault

- [D] Data / Information
- [D.e-files] encrypted data files
- [S] Services
- [S.prov] provided by us
- [S.prov.int] internal (users and means belong to the organization)
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.2] Data stored: ARIESProofingID, IDProofingSessionID, DocType, hash of document data, [optional Signed document data [optional with face picture], timestamp, virtul issuer identifier, ID proofing client InstanceIdentifier.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design
- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [IdP_IS_IdProofing] ID proofing service

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]

[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

6.1.4.7 [IdP_IS_BioEnrol] Biometric enrolment service

- [D] Data / Information
- [D.e-files] encrypted data files
- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.1] This service allows a user to be registered in the system through its biometrics, and therefore, providing a high level of assurance when the user/SPs demand authentication through biometrics to access a particular service.

[D3.2] The Biometric enrolment step collects private biometric information needed for the future authentication. The feature collected depends on policy, by default the service should use facial recognition, because it allows ID Proofing and may leverage on information already collected during the ID Proofing step.

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

In case multiple biometric enrolments are processed, each of them are independent and no link could be done by the server.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [IdP_UserEnrol] ARIES user enrolment process

Below (assets on which this one depends on)

- [IdP_IS_BioEnrol_Vault] Biometric enrolment service individual service vault
- [IdP_IS_Vault] ARIES secure vault service
- [User_IS_BioEnrol] Biometric enrolment client
- [User_IS_IssuanceMan] Issuance manager

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data	[4](13)	[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

6.1.4.8 [IdP_IS_BioEnrol_Vault] Biometric enrolment service individual service vault

- [D] Data / Information
- [D.e-files] encrypted data files
- [S] Services
- [S.prov] provided by us
- [S.prov.int] internal (users and means belong to the organization)
- [SW] Software
- [SW.std] standard (off the shelf)
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.2] Data stored: ARIESBioID, IssuanceSessionID, Signed Document Data, [Optional ARIESProofingID], timestamp, virtual issuer identifier, bio enrolment client InstanceIdentifier.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design
- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [IdP_IS_BioEnrol] Biometric enrolment service

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

6.1.4.9 [IdP_IS_Vault] ARIES secure vault service

- [D] Data / Information
- [D.log] activity log
- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.1] A remote service to store evidence collected during enrolment (in particular from the proofing phase). It would offer basic CRUD features (Create, Read, Update, and Delete), for the data stored by a user, and for managing the vaults by an administrator.

[D3.2, figure 6] Store log (IssuanceSessionID, ARIESBioID, [optional ARIESProofingID]

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design
- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [IdP_IS_BioEnrol] Biometric enrolment service
- [IdP_IS_vIDIssuance] Virtual identity issuance

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]

[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data	[7](3)	[7]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

6.1.4.10 [IdP_IS_vIDIssuance] Virtual identity issuance

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.1] Back-end application responsible for provisioning and management of main user Virtual ID (a.k.a. ARIES token). In a first implementation, the ARIES vID is being based on classical PKI digital signature and certificate, so that the issuance service interacts with the Certification Authority, which is the entity that actually generates the x.509 certificates. In the pilot stages of the project the Mobile ID is created relying on Mobile PKI using as baseline the IP proofing authentication performed previously. Nonetheless, this issuer service may also be implemented by other privacy-preserving technologies. This issuance process is part of the enrolment stage, and it is done after the user had performed successfully both the ID proofing process and the biometric enrolment.

Virtual Identity Issuer is a web application responsible for issuance of new virtual IDs, it is a centre piece of the system where all parts of the information are linked: it binds ID proofing and biometric verification transactions to a new virtual ID. Both biometric verifier and ID proofing must be trusted by the Issuer so it does not need to perform any additional verifications of user information by itself.

[D3.2] The vID issuance issues new credentials for the user based on the information from ID Proofing step. Private information disclosed to the service contains: - Data read from electronic document (depending on policy). Transparency may be improved by giving the user the possibility to review and limit the information disclosed. - Information the user is willing to submit. These user attributes have low level of assurance (only self-claimed), but may be used for convenience. The list is not limited, but in general may contain email, post address, phone number. The service creates the credentials including user attributes and sends the credentials to the user. The information is not persisted in the vID Issuance service and the audit log persisted in Secure Vault should contain only pseudonymous reference of the newly created credentials (ARIES ID).

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design
- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [IdP_UserEnrol] ARIES user enrolment process

Below (assets on which this one depends on)

- [IdP_IS_Vault] ARIES secure vault service
- [IdP_IS_vIDIssuance_Vault] Virtual identity issuance individual service vault
- [User_IS_vIDCreation] vID creation client
- [User_IS_IssuanceMan] Issuance manager
- [IdP_SS_CA] Certification service

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data	[1](14)	[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

6.1.4.11 [IdP_IS_vIDIssuance_Vault] Virtual identity issuance individual service vault

- [D] Data / Information
- [D.e-files] encrypted data files
- [keys] Cryptographic keys

- [keys.x509] public key certificates
- [S] Services
- [S.prov] provided by us
- [S.prov.int] internal (users and means belong to the organization)
- [SW] Software
- [SW.std] standard (off the shelf)
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.2] Store ARIESderivedID, CreationSessionID, partial credentials [?], attributes, timestamp, virtual issuer identifier, vID creation client InstanceIdentifier.

Information sources

- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [IdP_IS_vIDIssuance] Virtual identity issuance

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

6.1.4.12 [IdP_IS_vIDVerifier] vID verifier service

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.1] This component is in charge of verification of the ARIES vID: the user authentication. When a higher level of assurance is demanded, this service can communicate with the biometric verifier service to request the authentication of the user through biometrics. In case of the traditional approach is adopted, it can perform basic authentication through traditional PKI and using SAML, interacting with the vID AuthN client module in the user smartphone. In addition, the vID Verifier service can verify derived partial virtual identities. The approach or implementation for derivation, proving and verification the partial vID is open and can be based, among others, on SAML tokens (attribute-authentication

assertions) or by means of ABC-related proofs. For some optional scenarios, this vID Verifier service may be directly deployed in the service provider, so that the user can communicate directly with the SP in a M2M fashion. This approach avoids contacting the external IdM verifier service (managed by a third entity) in every request, which, in turn, avoids the IdM to trace the user's behaviour. The vID Verifier service must trust the Issuance Service; indeed, these two services will be usually managed by the same entity. Besides that, the verifier service must trust the biometric verifier in case this strong authentication is also required during the vID verification.

vID Verifier plays in the architecture role of the conventional Identity provider for Relying parties. It is the only entity authorized to access the virtual ID data directly. It is responsible for verification of the ID on one side, on the other side it is responsible to make sure only authenticated and authorized Service Providers may request the verification, and that the SPs are provided only the information they are authorized for.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [IdP_UserAuth] ARIES user authentication process
- [IdP_UserBioAuth] ARIES user authentication process with biometrics

Below (assets on which this one depends on)

- [User_IS_vIDAuthN] vID AuthN client

Value

dimension	value	accumulated values
[A] Availability		[7]
[I] Integrity		[6]
[C] Confidentiality		[5]
[Auth] Authenticity of users and information		[6]
[Acc] Accountability of service and data		[6]
[PD] Personal data	[1](14)	[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

6.1.4.13 [IdP_IS_BioVerifier] Biometric verifier service

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.host] hosts

Security domain

- [base] Identity Provider

Description

[D3.1] This component is in charge of the biometric authentication of the user by interacting with her/him through the smartphone app, to capture a fresh and live biometric image and execute the comparison with biometric reference collected during enrolment. This process is done during the vID verification stage in response to a request coming from the vID Verifier service. It should be noticed, that the verification process requires the user to be beforehand enrolled by the Biometric Enrolment

service. In general these two services are often managed by the same entity. As a result of the biometric verification, a new authentication assertion is sent back to the vID Verifier, during the same session.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [IdP_UserBioAuth] ARIES user authentication process with biometrics

Below (assets on which this one depends on)

- [User_IS_BioAuthN] Biometric AuthN client

Value

dimension	value	accumulated values
[A] Availability		[7]
[I] Integrity		[6]
[C] Confidentiality		[5]
[Auth] Authenticity of users and information		[6]
[Acc] Accountability of service and data		[6]
[PD] Personal data	[4](15)	[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.14 [User_IS_IDProofing] ID proofing client

- [D] Data / Information
- [D.e-files] encrypted data files
- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [User] ARIES User

Description

[D3.1] This module is in charge of interaction with the IdP Proofing service for vetting the user through the biometrics included in the breeder document. The role of ID Proofing client is to collect evidences (here chip data, and biometric data) and to communicate with the ID Proofing service to check authenticity of the data and consistency of the content (in particular biometric data within the chip matches with captured biometric data). This library, and the breeder document verifier library, are usually provided by the same organization as this client library relies on the former to perform to access to the chip contained in the breeder document.

[D3.2] The ID Proofing starts with an anonymous request from the App to the ID Proofing service. The service collects following private information: - Data read from the electronic document (face image, age, name, document id). The full scope of the reading depends on policy of the reading. - Face image from live capture.

All the data are processed on server-side for trust reasons: - Checking data signature through passport Public Key Directory - Checking data signature through the public key of the issuing authority of the eID

document - Checking live face capture against the reference portrait extracted from the electronic document

Once the data are verified, they are signed and encrypted by the service and sent back to the client. There is no data persistence in server-side, besides audit log information stored in Secure Vault with very limited scope (document id).

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design
- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [IdP_IS_IdProofing] ID proofing service

Below (assets on which this one depends on)

- [User_IS_DocVerifier] Breeder document verifier
- [User_IS_SWallet] Secure mobile wallet

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.15 [User_IS_DocVerifier] Breeder document verifier

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [User] ARIES User

Description

[D3.1] This component is in charge of dealing with different electronic documents during enrolment of new ARIES vID; it is the interface between the document and the ARIES ecosystem. It is in charge of reading and verification of the breeder document through NFC technology.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [User_IS_IDProofing] ID proofing client

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.16 [User_IS_BioEnrol] Biometric enrolment client

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [User] ARIES User

Description

[D3.1] This library allows interaction with the Biometric Enrolment service in order to register the user in the system. This client also interacts with the mobile wallet to obtain the user's biometric data required for authentication.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [IdP_IS_BioEnrol] Biometric enrolment service

Below (assets on which this one depends on)

- [User_IS_SWallet] Secure mobile wallet

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.17 [User_IS_vIDCreation] vID creation client

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [base] Identity Provider

Information sources

- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [IdP_IS_vIDIssuance] Virtual identity issuance

Below (assets on which this one depends on)

- [User_IS_SWallet] Secure mobile wallet

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.18 [User_IS_IssuanceMan] Issuance manager

- [S] Services
- [S.prov] provided by us
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [User] ARIES User

Description

[D3.1] This module is responsible for interaction with the Identity Issuer service during the enrolment stage in order to obtain the vID. In a traditional issuance process, it is able to generate Mobile PKI key pairs, and send the CSR to the Issuer.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [IdP_IS_IdProofing] ID proofing service
- [IdP_IS_BioEnrol] Biometric enrolment service
- [IdP_IS_vIDIssuance] Virtual identity issuance

Value

dimension	value	accumulated values
[A] Availability		[4]
[I] Integrity		[5]

[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[5]
[Acc] Accountability of service and data		[5]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.19 [User_IS_SWallet] Secure mobile wallet

- [D] Data / Information
- [D.e-files] encrypted data files
- [D.conf] configuration data
- [D.password] credentials (e.g. passwords)
- [D.auth] credential validation data

- [keys] Cryptographic keys
- [keys.com] protecting communications
- [keys.com.authentication] keys for authenticating
- [keys.x509] public key certificates
- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [SW] Software
- [SW.std] standard (off the shelf)
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [User] ARIES User

Description

[D3.1] It stores cryptographic keys, pseudonyms, ARIES vIDs (tokens) and biometric data. The wallet content is encrypted and its access is protected, so that only the local aforementioned trusted libraries can access to the secure wallet. The App may be shared among a group of users so it must provide separate partitions for their identities, each of them protected by different credentials (PIN/Pattern, biometry). Each implementation of the wallet must also allow storage of multiple vIDs and user must have a full control over information sharing. If one identity is selected no information about other must be disclosed to any service.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design
- [D3.2] D3.2. Virtual identity developments

Above (assets that depend on this one)

- [User_IS_IDProofing] ID proofing client
- [User_IS_BioEnrol] Biometric enrolment client
- [User_IS_vIDCreation] vID creation client
- [User_IS_vIDAuthN] vID AuthN client

Value

dimension	value	accumulated values
[A] Availability		[7]
[I] Integrity		[7]
[C] Confidentiality		[7]
[Auth] Authenticity of users and information		[7]
[Acc] Accountability of service and data		[6]

[PD] Personal data	[7](3)	[7]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.20 [User_IS_IdSelector] Identity selector

- [S] Services
- [S.prov] provided by us
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [User] ARIES User

Description

[D3.1] It is able to communicate with the SP provider to agree which particular attributes are needed to access to a particular service offered by the SP. Then the selector allows choice of the suitable partial identity that holds the minimum set of personal attributes according to the info required by the SP.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [User_IS_vIDAuthN] vID AuthN client

Value

dimension	value	accumulated values
[A] Availability		[7]
[I] Integrity		[6]
[C] Confidentiality		[5]
[Auth] Authenticity of users and information		[6]
[Acc] Accountability of service and data		[6]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.21 [User_IS_BioAuthN] Biometric AuthN client

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [S.prov.idm] identity management
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [User] ARIES User

Description

[D3.1] This mobile library is responsible for biometric authentication on the client side. To this aim, it captures fresh biometric data and, by interacting with the biometric verifier service, authenticates the captured data with the biometric reference that has been stored in the mobile wallet during enrolment. This strong authentication is performed in case the SP or the user requires a higher level of assurance. This authentication is done after the vID verification and authentication.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [IdP_IS_BioVerifier] Biometric verifier service
- [User_IS_SWallet] Secure mobile wallet

Value

dimension	value	accumulated values
[A] Availability		[7]
[I] Integrity		[6]
[C] Confidentiality		[5]
[Auth] Authenticity of users and information		[6]
[Acc] Accountability of service and data		[6]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.1.4.22 [User_IS_vIDAuthN] vID AuthN client

- [S] Services
- [S.prov] provided by us
- [S.prov.ext] external users (under contract)
- [SW] Software
- [SW.std] standard (off the shelf)
- [SW.std.other] other ...
- [HW] Hardware
- [HW.mobile] mobile equipment, portables, ...

Security domain

- [User] ARIES User

Description

[D3.1] It allows interaction with the vID Verification service in order to authenticate the user. This process is triggered by the SP when a user wants to access a service. In a first ARIES prototype it is a Mobile ID app, implementing the vID functionality as authentication device relying on a PKI.

Information sources

- [D3.1] D3.1. ARIES eID ecosystem technical design

Above (assets that depend on this one)

- [IdP_IS_vIDVerifier] vID verifier service

Below (assets on which this one depends on)

- [User_IS_SWallet] Secure mobile wallet
- [User_IS_IdSelector] Identity selector

Value

dimension	value	accumulated values
[A] Availability		[7]
[I] Integrity		[6]
[C] Confidentiality		[5]
[Auth] Authenticity of users and information		[6]
[Acc] Accountability of service and data		[6]
[PD] Personal data		[5]

(1) [4] 4 hours < RTO < 1 day

(2) [4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(3) [7] Maximum: Those interested will find significant or even irreversible consequences, which may not be overcome.

(4) [5] is likely to cause significant distress to an individual
[4] Significant: Those interested will find significant consequences, which should be overcome without serious difficulties.

(5) [5] is likely to cause significant distress to an individual
[5] is likely to cause a significant breach of a legal regulatory requirement for personal information
[4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

(6) [5] is likely to cause a significant breach of a legal regulatory requirement for personal information

(7) [3] is likely to cause distress to an individual
[7] RTO < 4 hours

(8) [3] is likely to cause a breach of a legal or regulatory requirement for personal information

(9) [7] RTO < 4 hours

(10) [6] is likely to cause significant distress to a group of individuals

(11) [5] is likely to cause significant distress to an individual

(12) [1] Limited: Interested parties may find non-significant inconveniences.

(13) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.
[4] The rights and freedoms of the interested parties are assaulted, for example, a judicial summons, entering into a list of delinquency or disclosure of personal data with significant impact on the reputation of the interested party.

(14) [1] Extra costs, denial of access to some services or breach of material obligations with economic losses.

(15) [4] Undue appropriation of funds, loss of employment or breach of material obligations with relevant economic losses.

6.2 *Potential accumulated risk*

For each valuated asset, PILAR applies a threat catalogue – including an estimated probability and impact – and generates a potential accumulated risk. Potential risk means the risk that exists before the application of any countermeasures to mitigate it.

asset	[A]	[I]	[C]	[Auth]	[Acc]	[PD]
ASSETS	{5.9}	{5.4}	{6.3}	{6.8}	{5.1}	{4.8}
[B] ARIES Processes						{4.8}

[IdP_UserEnrol] ARIES user enrolment process						{4.8}
[IdP_UserAuth] ARIES user authentication process						{3.6}
[IdP_UserBioAuth] ARIES user authentication process with biometrics						{4.8}
[IS] Information services	{5.9}	{5.4}	{6.3}	{6.8}	{5.1}	
[IdP_IS] ARIES identity provider's IS	{5.9}	{5.1}	{6.3}	{5.7}	{5.1}	
[IdP_IS_UserWebEnrol] Enrolment web application	{4.2}	{3.7}	{5.1}	{3.9}	{4.5}	
[IdP_IS_IdProofing] ID proofing service	{4.2}	{4.2}	{6.3}	{5.7}	{4.5}	
[IdP_IS_IdProofing_Vault] ID proofing service individual service vault	{4.2}	{4.2}	{6.3}	{5.7}	{4.5}	
[IdP_IS_BioEnrol] Biometric enrolment service	{4.2}	{4.2}	{6.3}	{5.7}	{4.5}	
[IdP_IS_BioEnrol_Vault] Biometric enrolment service individual service vault	{4.2}	{4.2}	{6.3}	{5.7}	{4.5}	
[IdP_IS_Vault] ARIES secure vault service	{4.2}	{5.1}	{6.3}	{5.7}	{4.5}	
[IdP_IS_vIDIssuance] Virtual identity issuance	{4.2}	{4.2}	{5.1}	{3.9}	{4.5}	
[IdP_IS_vIDIssuance_Vault] Virtual identity issuance individual service vault	{4.2}	{4.2}	{6.3}	{5.7}	{4.5}	
[IdP_IS_vIDVerifier] vID verifier service	{5.9}	{4.8}	{3.3}	{4.5}	{5.1}	
[IdP_IS_BioVerifier] Biometric verifier service	{5.9}	{4.8}	{3.3}	{4.5}	{5.1}	
[User_IS] ARIES user's IS	{5.9}	{5.4}	{6.3}	{6.8}	{5.1}	
[SS] Outsourced services	{2.8}	{3.4}	{4.5}	{3.3}	{3.9}	

6.3 *Information security measures*

To reduce potential risk, any solution based in ARIES should adopt a standard set of technical and organizational information security measures:

aspect	top	safeguard	doubts	source	comment	recommendation
		SAFEGUARDS				
M	EL	[IA] Identification and authentication				8
T	EL	[AC] Logical access control				7
M	PR	[D] Protection of Data / Information				6
M	EL	[K] Protecting cryptographic keys				9
M	PR	[S] Protection of Services				6
M	PR	[SW] Protection of Software				7
M	PR	[HW] Protection of Hardware				7
M	PR	[COM] Protection of Communications				
M	PR	[IP] Logical border protection system				
M	PR	[MP] Protection of Media				
M	PR	[AUX] Auxiliary Means				5
PHY	EL	[HW_0049] Physical protection of equipment				6
PHY	PR	[L] Protection of the installations				
PHY	EL	[PPS] Perimeter protection				
PER	PR	[PS] Personnel				6
M	PR	[PDS] Potentially dangerous services				
M	CR	[IR] Incident management (ICT)				6
T	PR	[tools] Security tools				8
M	CR	[V] Vulnerability management				6
T	MN	[A] Logging and audit				6
M	RC	[BC] Business continuity (contingency)				5
M	AD	[G] Organisation				6
M	AD	[E] External Relations				6
M	AD	[NEW] Acquisition / development				4

The column Recommendation signals the most important safeguards to apply when deploying the ARIES based solution. When a set of safeguards is not particularly relevant, the corresponding cell appears in grey colour.

Not surprisingly, the top recommendations refer to cryptographic key protection, identification and authentication measures and implementation of specific security tools, specifically against malware.

6.4 *Current accumulated risk*

The tool also offers the residual accumulated risk, assuming the aforementioned standard set of technical and organizational security measures are applied when implementing the solution, as well as specific measures in case of personal data. As we can see, if an ARIES based solution applies these measures, residual risk may be acceptable under GDPR.

asset	**[A]**	**[I]**	**[C]**	**[Auth]**	**[Acc]**	**[PD]**
ASSETS	{3.2}	{2.9}	{3.9}	{4.4}	{2.6}	{3.8}
[B] ARIES Processes						{3.8}
[IdP_UserEnrol] ARIES user enrolment process						{3.8}
[IdP_UserAuth] ARIES user authentication process						{2.6}
[IdP_UserBioAuth] ARIES user authentication process with biometrics						{3.8}
[IS] Information services	{3.2}	{2.9}	{3.9}	{4.4}	{2.6}	

[IdP_IS] ARIES identity provider's IS	{3.2}	{2.6}	{3.9}	{3.4}	{2.6}	
[IdP_IS_UserWebEnrol] Enrolment web application	{1.4}	{1.3}	{2.7}	{1.6}	{2.1}	
[IdP_IS_IdProofing] ID proofing service	{1.5}	{1.9}	{3.9}	{3.4}	{1.9}	
[IdP_IS_IdProofing_Vault] ID proofing service individual service vault	{1.5}	{1.9}	{3.9}	{3.4}	{1.9}	
[IdP_IS_BioEnrol] Biometric enrolment service	{1.5}	{1.9}	{3.9}	{3.4}	{1.9}	
[IdP_IS_BioEnrol_Vault] Biometric enrolment service individual service vault	{1.5}	{1.9}	{3.9}	{3.4}	{1.9}	
[IdP_IS_Vault] ARIES secure vault service	{1.5}	{2.6}	{3.9}	{3.4}	{1.9}	
[IdP_IS_vIDIssuance] Virtual identity issuance	{1.4}	{1.9}	{2.7}	{1.6}	{2.0}	
[IdP_IS_vIDIssuance_Vault] Virtual identity issuance individual service vault	{1.3}	{1.7}	{3.7}	{3.2}	{1.7}	
[IdP_IS_vIDVerifier] vID verifier service	{3.2}	{2.4}	{0.98}	{2.1}	{2.6}	
[IdP_IS_BioVerifier] Biometric verifier service	{3.2}	{2.4}	{0.98}	{2.1}	{2.6}	
[User_IS] ARIES user's IS	{3.1}	{2.9}	{3.9}	{4.4}	{2.6}	
[SS] Outsourced services	{0.76}	{0.91}	{1.8}	{0.90}	{1.1}	

7 Recommendations

Our ethical and data protection analysis, including the information security issued, shows the need to apply some guidance when implementing a new solution based in the ARIES ecosystem. Otherwise the solution may not offer an adequate level of protection, even if based in a set of components specifically designed and appropriate for this objective.

The main recommendations are the following:

- The solution should conduct a detailed ethical assessment to avoid all forms of discrimination, in particular considering the impact of not having access to the technical elements needed to participate in the electronic services.

- The solution should separate as much as possible the operation of the different components in diverse providers, because if a unique provider operates all components it may have the same access to information as in a classical centralized approach.

- The solution should apply biometric authentication just when strictly needed, and with a proper legal basis, aligned with Article 9 GDPR or National legislation. As the legal basis for biometric data processing is very limited, it may be needed to implement the solution based in consent.

- Providers implementing the solution should implement a specific set of information security safeguards, to maintain the residual risk at an acceptable level. Otherwise it may be impossible to prove compliance with GDPR.

- Providers implementing the solution must implement the legal controls required my GDPR and National legislation, including producing a specific data protection impact report and consulting with the national authority before starting the processing of data.

8 References

- Catalan Data Protection Authority. *Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)*. Version January 2018

- Council of the European Union: *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration*) Interinstitutional File: 2017/0352 (COD), 1938/18, 23 May 2018.

- European Commission. Directorate-General for Research & Innovation. H2020 Programme. *Guidance: How to complete your ethics self-assessment*. Version 5.2. 12 July 2016.

- European Data Protection Supervisor (EDPS): *Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents*. Version August 2018

- ISO/IEC: *Information technology-Security techniques – Guidelines for privacy impact assessment*. Version June 2017

- Spanish Data Protection Agency. *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*.

- Spanish Data Protection Agency. *Guía práctica para Evaluaciones de Impacto en la Protección de datos sujetas al RGPD*.

- Statewatch (2017) *EU-wide biometric databases, 'soft targets', cybersecurity and data protection : Commission's fourth report on building the 'Security Union*', Briefing by C. Jones, Feb. 2017.

- Taylor, E. (2016): 'Mobile payment technologies in retail: a review of potential benefits and risks', *International Journal of Retail & Distribution Management* (44:2) 159-177.

- Working Party Article 29: *Guidelines on Data Protection Impact Assessment (DPIA)*. Version October 2017.

- Working Party Article 29: *Opinion 3/2012 on developments in biometric technologies*. Version April 2012.