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

ARIES
"reliAble euRopean Identity EcoSystem"

D5.1 – Initial Business and Exploitation Plan

Due date of deliverable: 31-05-2018
Actual submission date: 31-05-2018

Start date of project: 1 September 2016 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	

D5.1 – ARIES Initial Business and Exploitation Plan

Editor
Aljosa Pasic (Atos)

Contributors
Saher, GTO, ATOS, UMU, ERTZ, OPCC, Sonae

Reviewers
SONAE

30-05-2018
Version 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
0.01	29/11/2017	Aljosa Pasic (Atos)	Table of Contents
0.1	20/12/2017	Aljosa Pasic (Atos)	First draft
0.2	06/02/2018	Aljosa Pasic (Atos)	Second draft
0.3	27/04/2018	Aljosa Pasic (Atos)	Third draft, includes individual exploitation plans and section from UMU on privacy preserving technologies
0.4	08/05/2018	Aljosa Pasic (Atos)	Fourth draft, editing previous inputs
0.5	17/05/2018	Aljosa Pasic (Atos)	Integration of contributions from partners
0.6	29/05/2018	Thiago Costa (Sonae)	Peer review of deliverable
1.0	30/05/2018	Aljosa Pasic (Atos)	Final version ready for delivery

Executive Summary

This document is presenting initial ARIES business and exploitation plans, covering both individual (annex 1) and the joint exploitation plans. It is introducing the main ARIES concepts and terminology used, based on architectural choices, but also relevant exploitation strategy, namely to make overall system as modular and flexible as possible. The description of project results, from the highest to the lowest level of abstraction is given with the introduction to the packaging strategy that is going to be finalised in the last phase of the project, once that market assessment findings and initial exploitation assumptions have been validated.

The analysis of business and the other market stakeholders (e.g. regulators) is done with few examples from the adjacent or underlying identity ecosystems. These cover:

- eIDAS identity ecosystem built on top of so called "notified e-ID schemes" recently introduced and supported by eIDAS regulation
- ICAO/IATA identity ecosystem where we basically refer to travel identity document (e-ID card or ePassport) and related documents or attributes such as boarding pass
- Use of e-ID in eCommerce, which is not limited to, but uses heavily social network login as an example of the third party e-ID

Identification of target audience segments, value proposition, channels, cost structure and potential business models with revenue streams is done from February 2018 to May 2018 and will be continued until the end of the project. The initial findings from the evolution of identity ecosystem are that there is a strong demand for the identity proofing and verification (IPV) detached from the other phases of e-ID lifecycle (e.g. issuance, authentication, management). Many enterprises are busy with identity proofing upgrades or replacements to their current solutions, including the leading social network or online service providers. General Data Protection Regulation (GDPR) has finally come into force and this is also experienced by many users that receive regularly policy updates from identity and service providers. Service providers and citizens are both adopting mobile ID very fast. For service providers, reducing customer abandonment and avoiding face to face verification are the main drivers for change, while simultaneously improving the customer experience and opening new channels, is a clear argumentation for adopting mobile ID. On citizens' side, convenience drives adoption, but it has been also acknowledged the importance of privacy preserving solutions. As for law enforcement authorities, there is a need to build better argumentation and provide use cases of approaches that reduce the risk of fraud, maybe inspired on the physical identity fraud. All these multi-stakeholder interests are not easy to be met at the same time, with one single solution. In addition, non-technical issues, including legal, ethical or socio-economic (e.g. trust, attitudes, perceptions), need to be taken into account. Unlike other business e-ID is still partially private, partially public, business and strong partnerships are likely to emerge in order to meet these multiple demands and requirements. Examples already exist in Scandinavia (several Bank ID ecosystems) and more recently Switzerland or Germany.

While demand side analyses ends up with challenges, opportunities and threats, supply side analysis also delivers findings that help ARIES in identifying some of its strengths or weaknesses, as well as to position itself in this competitive market. Three ARIES partners are, in a matter of fact, already very well positioned in the e-ID market, so the analysis is also introspective in a sense that individual exploitation plans needs to take into account existing solutions and strategies. This makes ARIES positioning a multi-iteration process that will be further calibrated in the final deliverable. Individual exploitation plans and SWOT analyses were used for the first draft of the joint exploitation plan. The plan is introducing possible business opportunity driven set-up with differentiated roles for technology providers and service providers, such as consultants and integrators that would pick up ARIES components from the catalogue and use "mix and match" approach to develop specific offering for the client. The business set-up would be complemented by sales role that can rely on existing or new marketing channels.

Contents

List of Figures

List of Tables

1 Introduction

The need for harmonized and improved approach to the issuing and derivation processes of electronic identity based on highly trustworthy physical documents that meet certain minimum security and content standards is one of the key priorities for raising the level of trust in digital services. Whether it comes to digital single market in Europe, digital transformation of certain industries, or cyber-physical convergence, there are currently many concerns about identity-related crimes, as well as other issues such as preservation of privacy. While one type of project or initiatives is seeking to effectively combine biometric technologies with eID processes, in particular in relation to issuance of breeder documents, the others are more concerned about usability and privacy, especially in mobile identity ecosystems.

ARIES is ambitious project and it tackles many of these issues. It promotes the use of national and trusted identities like eID and ePassport as a baseline for citizen digital life credentials that can demonstrably offer high level of security against identity-related crimes. Its main technical contribution consist of integration of separated modules to assemble a secure system able to derive virtual identities considering different levels of assurance for different purposes, with an option to support privacy-preserving capabilities, including selective attribute release. It also targets proactive support to law enforcement authorities by adding mechanism to prevent identity fraud, so called secure vault. In regard to usability through mobility, it enables mobile ID and integrates a number of specific technologies, for example a Secure Mobile Wallet to securely and conveniently store and access virtual Mobile ID. ARIES also includes sector and use case specific integration, deployment and configuration, where the overall system is ready for operational use. This is what we call “ARIES platform” with two ongoing examples in pilots: e-Commerce and Smart Airport (note: this deliverable is using term “Smart Airport” to refer to “identity virtualisation in airports” pilot).

While of these issues are linked to some of presumed differentiators, benefits or competitive advantages, the aim of this deliverables is to streamline these into identified and well-presented value propositions that could be further used for selling propositions. It could be too arrogant to say that all of these value and selling propositions are unique, but the uniqueness of ARIES approach lies in the integration of so many previously separated advances in e-ID research and innovation. Security and usability, traceability and privacy, all balanced in a solution where strength and opportunities outweighs weaknesses and threats.

In order to get to the market, this deliverable takes a closer look at related market from demand and supply side. It is also making comparative assessment of similar solutions and alternatives, as well as possible packaging strategy for the project results. As the success and overall impact often relies on correct positioning, the large part of effort here is spent on related considerations. Finally, the individual partner interest, motivations etc. are collected before the joint exploitation and business plan is drafted.

1.1 Purpose of the document

The main purpose of this document is to provide elements of the exploitation and future business plan for ARIES results. This includes overall result, which is ARIES system, as well as components of it (software modules) or intangible results such as knowledge or experience in deployment of the system. It serves as the main line of project work related to the post-project activities, such as policy and market impact. The final version of this deliverable is envisaged in January 2019 and will contain validation of several assumptions contained in this document, as well as additional progress in activities already started, such as partners agreements regarding the hypothetical revenue sharing.

1.2 *Relation to other project work*

In particular, D5.1 is closely related to the following deliverables:

- **D7.2 Innovation plan**

  It presented theoretical background relevant for ARIES innovation and outlined initial strategy. Most of the theoretical work refers to innovation in a single organisation and for this reason innovation management process had to be adapted with the specificities of ARIES consortium where three industrial partners already have large portfolio of solutions in electronic identity management market. This sets initial context and constraints some options since most of results are built on the top or proprietary technology. Initial set of ideas is based on technical outcomes and will be used for this deliverable D5.1. After the first draft and SWOT analysis, the list of ideas will be extended with business innovation ideas and other factors (legal, societal) in order to feed innovation funnel. Biometric verification component, for example, might be offered as an external service to ARIES identity provider, while innovative application in a different scenario (e.g. hotel chain or rent a car) could be selected as an idea worth to explore. Therefore, several iterations of innovation process will have to be done during the last year of the project in order to complete collaborative assessment and prioritisation task and provide final feedback for D5.2.

- **D5.4 Final Communication Plan and Activities Report**

  This report will report communication and dissemination activities of ARIES and the planned activities, including the marketing activities.

- **D6.1 First Dissemination, Standardization Activities Report**

  Report documenting the dissemination, clustering and standardization activities of the project partners during the first half of the project, includes some activities relevant for business opportunities.

1.3 *Acronyms used in this document*

SWOT	Strengths, Weakness, Opportunities, Threats
eID	Electronic Identity
eIDAS	Electronic identification and trust services
ABC	Attribute based credentials (also automated border control)
LoA	Level of Assurance
OTP	One time password
NFC	Near Field Communication
PIA	Privacy Impact Assessment
vID	Virtual Identity
WP	Work Package

2 Methodology

The Deliverable contains different methodological approaches. The main methodologies used are typical for the exploitation of results in collaborative projects although some of them apply and are well known in a wider business planning context.

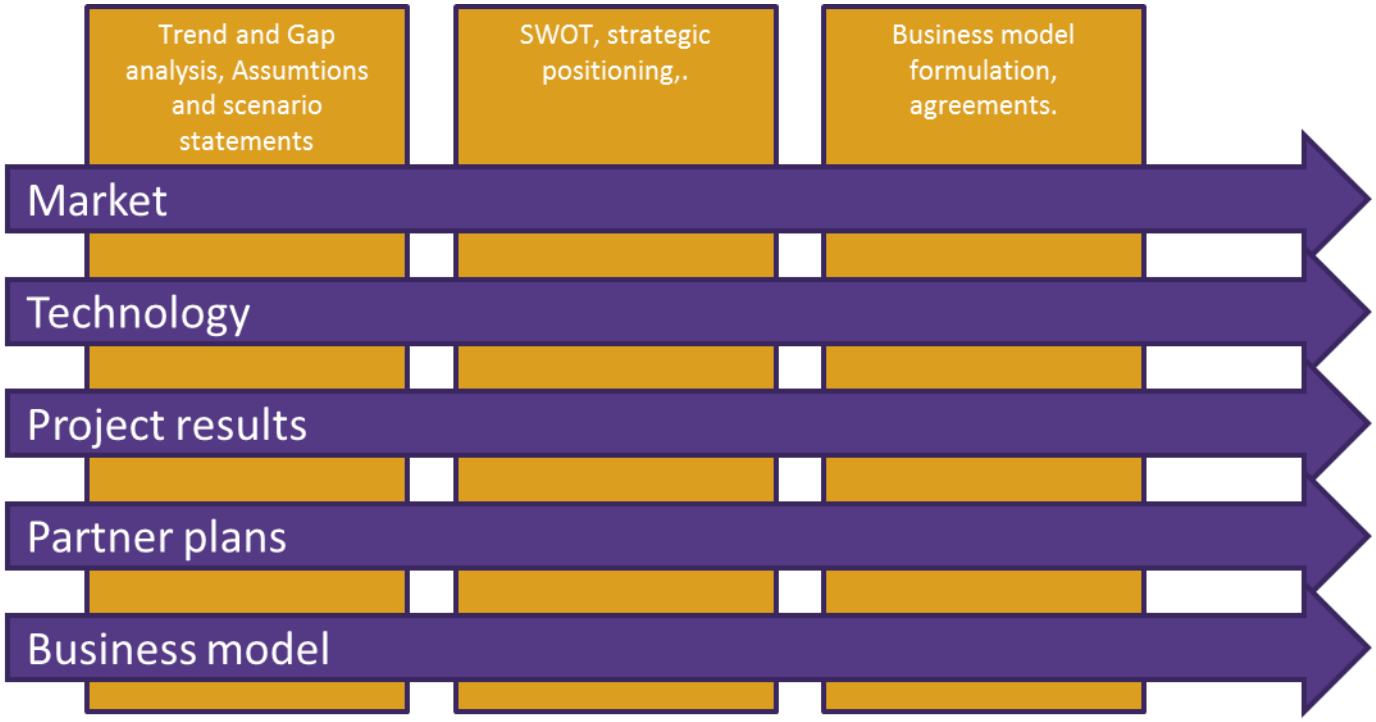


Figure 1: overview of main activity lines in the exploitation strategy

In figure above we depict the main lines of activities related to this deliverable for each one of these lines there are different methodologies to be applied. The selected approach was useful in order to start early and make parallel progress in each of the lines, as well as to provide feedback and receive comments from other work packages. While the approach takes elements from [1] and [2] , both of which apply to consortium-executed projects or networked organisations (in a hypothetical joint exploitation scenario), the implementation in this project is taking more opportunity-driven approach and is applying some external methodological elements, strategies or tools, including brainstorming or dedicated conference calls, to clarify issues and make convergence of points and perspectives.

Business Model Canvas, for example, is a strategic management and lean template for developing new or documenting existing business models and can be used either at the beginning of the project or, as it is case in ARIES, after the individual exploitation plans have been drafted. These plans are drafted with the use of specific template (see annex 1). In a similar way, SWOT (it is an acronym for strengths, weaknesses, opportunities, and threats analysis), is a structured planning method used as part of the exploitation planning process. SWOT analysis requires a team effort, and for this reason specific mini-brainstorming session was organized during the consortium meeting in Prague on March 15th 2018.

At the same time there is some interdependency with activities from the other work packages and methodologies applied there. Innovation Management methodology was described in D7.2 and it adopts elements from common methodologies such as Innovation funnel with Atos specific tools and methods such as Sandclock, developed by Atos in order to cross this “no man’s land” between research and market, and to address both “push” from research and “pull” from market. It follows discover-filtering-growth-market pattern in order to bring project results to the market. In general, all innovation activities which are excluded from technological innovation, such as business process innovation (e.g. verification process description from work

package 3), as well as marketing or organizational innovation, are converging into business and exploitation plan analysis, presented here. In particular, Act phase of strategy from D7.2 aims to "Evaluate the overall plan and improve it (if necessary) with the experience of the previous iterations, including acquiring feedback on i.e. the usability offered by the ARIES solutions". This version of deliverable has received some feedback from the first pilot, which was e-commerce, while the final version will also contain feedback from end users from the smart Airport scenario.

The use of different methodologies and interdependency with the other work packages is always in line with the project vision strategy, which is translated into number of project specific objectives, such as creation of eID ecosystem with ARIES system consisting of interchangeable and replaceable software modules and components. The technical approach, based on modular architecture, flexible integration strategies and open source licensing for integration APIs, is clearly in line with achieving sustainability of software results. ARIES ecosystem, as we will see in the following chapters, is socio-technical construction which cannot be achieved overnight and it needs gradual, but strong, commitment from the main stakeholders with citizens as the focal point of the strategy. A citizen-centric eID ecosystem is all about putting citizens at the core, and working backwards from their needs to technological and process innovation on their behalf, as well as definition of solutions that satisfy their needs, while elevating the overall security assurance level. However, service provider perspective should not be marginalized and we will try to learn from previous lessons related to the service provider adoption of e-identity solutions.

On the other hand, the sustainability factors for the project results have been clustered according to existing knowledge and perspectives of project partners. The aspects of legal sustainability, societal and ethical aspects are addressed elsewhere (work package 2) so the main focus here is on business sustainability and technical sustainability. Nevertheless, the business sustainability assesses the value of the service from an overarching perspective by including societal, policy, cybersecurity and macroeconomic gains of ARIES ecosystem. The technical sustainability analysis follows more focused approach starting from the existing market solutions, as well as communities which would benefit or could contribute to the project results sustainability strategy.

Various understandings of the project results exploitation are also reflected in the individual exploitation plans and result in divergences about the spectrum of activities that are considered after the project.

3 Project context and results

In ARIES grant agreement it was already mentioned that the project "focuses on the combination of technologies to provide a platform and ecosystem" suggesting several layers of abstraction, from the identity ecosystem, through platforms (in plural), all the way to the software components such as application programming interfaces, libraries and others that embed or implement novel technologies, techniques, algorithms etc. For this reason we will treat these different project results abstractions in a different way. Some of them might be "ready to sell", while the others will have strong dependency on internal (e.g. maintenance of related components) and external (e.g. other stakeholders) sustainability factors.

This deliverable focus is on "exploitable" results with the focus on tangible results with commercial value. The results such as know-how will be mentioned in the individual exploitation plans, while others (e.g. contribution to a consistent European identity strategy, approach to increase trust while retaining efficiency and convenience, contributions to privacy initiatives or strategy etc.) On the platform side ARIES provides components for mobile phone offering the citizen an efficient and convenient way to manage identities, including the possibility to anchor the trust on a secure element and infrastructure that will be used to derive virtual identities supporting different privacy preserving and anonymization capabilities. Furthermore, ecosystem is planning to cover multi-domain interaction where a single eID domain (e.g. telco, banking) is considered to be eID ecosystem on its own. In this sense, ARIES ecosystem could evolve towards a meta-ecosystem that crosses existing eID ecosystem borders.

As mentioned before, ARIES is not the first attempt to build user-centric ecosystem that gives effective control of citizens over their virtual identities, allowing them to enrol and build separate identities for different purposes. We need to take into account lessons learned and to enhance the previous models with new value and selling propositions, such as reduction of identity fraud through linking of ePassport/eID cards to virtual ID used in online services or for access to physical places.

3.1 *eID ecosystem*

The word ecosystem itself is frequently misused when combined with "digital" adjective. While in the "physical" world it represents a group of interconnected elements, formed by the interaction between them and with their environment, the definition of "digital ecosystem" is relatively new and it refers to "a distributed, adaptive, open socio-technical system with properties of self-organisation, scalability and sustainability".

Identity ecosystem definition, on the other hand, is often linked to a very specific proposal from the United States federal government to improve identity authentication on the Internet. This proposal, formally known as the National Strategy for Trusted Identities in Cyberspace, among its objectives wants to develop a comprehensive Identity Ecosystem framework. They define Identity Ecosystem as a user-centric online environment which is a set of technologies, policies and agreed upon standards that securely supports transactions ranging from anonymous to fully-authenticated and from low to high value.

As a socio-technical construction, ARIES ecosystem is still missing "socio" part, in other words a large uptake by the main stakeholders. For this reason, we must work with assumptions and idealize this eID ecosystem, while trying to compare its strengths and weaknesses. We will look at value vectors of ARIES ecosystem when it comes to privacy, convenience, efficiency, ease-of-use, security, confidence and choice, all of which are

considered essential by end consumers, whether we consider citizens or service providers in a multi-sided eID market.

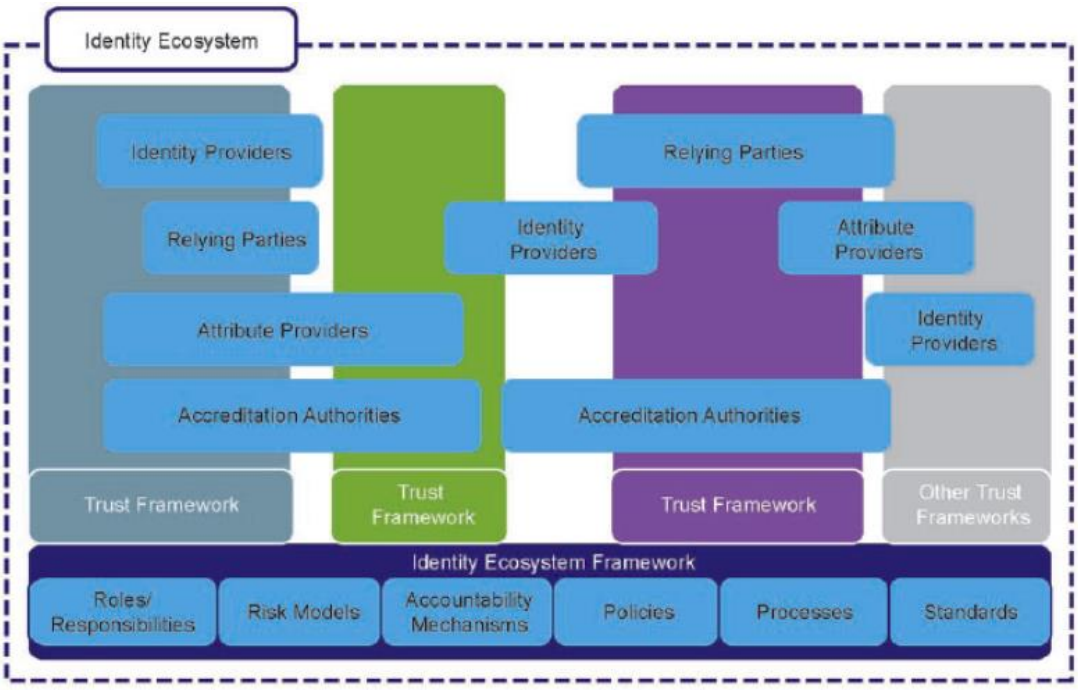
One of the novelty in ARIES is addressing the current gaps in identity ecosystems when it comes to identity fraud, which is then translated into business (i.e. financial loss) and societal (i.e. people trafficking) impacts. This gap is supporting mechanism for law enforcement in case of identity fraud, a mechanism that would link strong identity proof, such as eID or ePassport proofing and verification, with virtual eID (vID) used for authentication to specific service or access control providers. From a legal perspective, setting up an extended e-ID ecosystem implies a higher complexity of the relationships among all the concerned stakeholders, and this is analyzed in WP2 of ARIES. It is also essential to analyse the implications of this data processing from the perspective of the EU privacy legal framework and specify the role and responsibilities of each actor in ecosystem. eIDAS Regulation is providing already an excellent basis for cross-border identity ecosystem deployment, especially when private sector becomes aware of its advantages, but lacks maybe flexibility when it comes to large number of users, both citizens and service providers, that do not have need, or do not want, to rely on eID verification provided by governmental identity providers through eIDAS nodes. In this document, we also refer to eIDAS ecosystem as pan-European eID ecosystem to be created around what is referred as "notified" eID solutions in EU member states and related infrastructure, composed on national eIDAS nodes and links to IdP. Notified eID solutions refer to eID issued by the government, on behalf of government or under the control of government, but these do not necessarily need to be linked to unique identity number or implemented through smart card technology (eID card). ARIES is specifically designed for eID cards or ePassports, physical documents considered as "breeders" for ARIES virtual vID and therefore overlap only partially with eIDAS ecosystem at the moment (Belgium, Spain, Germany, Hungary, Latvia, Lithuania, Malta, Luxembourg and Slovakia have smartcard based eID in use, while many other countries have it in development phase). We expect this situation will change rapidly due to the recent (May 2018) EC proposal for a regulation on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

The second eID ecosystem that partially overlaps with ARIES is what we will call "ICAO eID ecosystem". The International Civil Aviation Organization is a specialized agency of the United Nations located in Montreal, Canada. ICAO standardization of data contained in passports started in the 80s with a machine-readable travel document (MRTD) where the data on the identity page is encoded in optical character recognition format. They are standardized by the ICAO Document 9303 (endorsed by the International Organization for Standardization and the International Electro technical Commission as ISO/IEC 7501-1) and have a special machine-readable zone (MRZ), which is usually at the bottom of the identity page at the beginning of a passport. More recently ICAO has also standardized biometrics used in ePassports such as facial recognition, fingerprint recognition, and iris recognition. Document and chip characteristics are documented in the ICAO Doc 93031 with biometric file formats and communication protocols to be used in passports. There are national ID cards that comply with ICAO9303 standard such is the case of Netherlands, so they could also be considered as a part of "ICAO eID ecosystem". In line with what was mentioned before (EC proposal for a regulation on strengthening the security of identity cards of Union citizens) we expect that a larger part of eIDAS eID ecosystem will overlap with ICAO eID ecosystem in the future. When it comes to ePassports, which are the basic pillar of "ICAO eID ecosystem" there are already more than 100 States and non-state entities (i.e. United Nations) currently issuing ePassports, and over 490 million ePassports in circulation. The increasing number of States issuing ePassports and the correspondingly high volume of ePassports being issued results in a highly complex ecosystem so that ICAO created a system to facilitate the sharing of information between States: the ICAO Public Key Directory (PKD), a kind of centralized directory that offers an cost-effective online source for up-to-date information.

[1] https://www.icao.int/publications/pages/publication.aspx?docnum=9303

Finally, the third eID ecosystem that will be analyzed in this deliverable and that is partially overlapping with ARIES, is the one used by e-commerce service providers. It is neither centralized nor single federated solution. With "eCommerce eID ecosystem" we will denominate a set of different solutions that enable citizen and business to use ecommerce online services. For this purpose service providers can implement their own identity management solution or can rely on external third party identity providers, often a social network based login, such as Facebook ID or Google ID. More recently a market subsegment called CIAM (consumer identity and access management) emerged representing a number of identity management solutions and scenarios, including brokers, that satisfy needs and requirements of online service providers, such as scalability or sharing of specific attributes.

ARIES ecosystem therefore overlaps with all these existing eID ecosystems. Rather than competing with them, it is enhancing them and it is building bridges. It is using eID cards or ePassports in the identity proofing and verification phase, while it is more similar to the current offerings of eID in eCommerce, when it comes to authentication and usage phase. Different derived or vID means can be used for different purposes, in order to increase security, safeguard better personal data and boost multi-party trust. Allowing access to eID card and ePassport identification data is one of the most relevant challenges solved in ARIES ecosystem. A chain of derived vID that progressively allows a higher level of anonymity, taking into account that access to data will be limited to those attributes strictly required, is another key result when it comes to flexibility and customer choice. Finally, better support for the law enforcement and strengthening the link between physical documents that contain eID or biometric data and what we define as virtual or derived (web and also mobile) identity, are further strengths and arguments that could be used in building the value and selling propositions in order to build full blown eID ecosystem.



Source: US NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE (2011)

Figure 2: identity ecosystem according to US national strategy

3.2 *System and platforms*

While any combination of software and/or hardware components is generally regarded as a "system", use of term "platform" has connotations closely related to the creation of specific digital "ecosystems". Term software platform was used to denote a software programming development environment with language, runtime, components and all associated libraries and binaries. Parallel to this term, software framework term was also used to describe a standard way to build and deploy applications, together with some ready to use code, so it can be understood as the part of a software platform enhanced with procedures and other support to facilitate or speed up development. More recently meaning of term platform evolved, as the development environments and different software products (e.g. applications, operating systems) converged, so that now Android, Facebook or SAP are all considered platforms. They all create network effects through interactions they enable, so they became "ecosystem enablers".

Stork was one of the first projects in Europe aiming at establishment of a European eID Interoperability Platform that will allow citizens to use national eID services across borders. This platform is further enhanced in many other projects (see previous chapters on eID ecosystems) and one platform of particular interest for ARIES is FutureID [21] platform, a kind of eID broker platform where user can select either low assurance, social login based eID, or high assurance, national card based eID. There is also the follow up project Future Trust that extends STORK (or present day eIDAS platform) with heterogeneous IDM technologies. However, in recent documents the terminology has changed and the network of Stork proxy servers (eIDAS nodes) is not anymore regarded as a "platform" but rather as an infrastructure with eIDAS "nodes" that are based on "reference implementations".

In line with this understanding of eID platform, and eID system or infrastructure, we will also define ARIES results. eID card or ePassports are necessary part of the overall infrastructure, in order to derive vID, but they are not components of the main ARIES system. This system, described in D3.1, integrates components able to derive virtual identities considering different levels of assurance, supporting privacy-preserving and anonymization capabilities, as well as including selective information release under control of users. Another distinguishing feature is a law enforcement supporting mechanism in case of identity fraud, contributing therefore to increase trust of users in the cyber-physical eID ecosystem. This main ARIES system is customised and deployed in two scenarios: eCommerce and Smart Airport. Since the use of components is very different in each use case, we use term "ARIES platforms", therefore distinguishing between eCommerce platform and Smart Airport platform.

The Mobile-Device based tools or apps for Automatic Document Verification needed to capture and verify the breeder documents are considered as a part of both platforms, as well as infrastructure necessary to produce the Virtual Identities. However, services or devices that consume identity services, or policies that apply, are different. Basically, depending on packaging, different collections of software components to create different technological solutions can be placed on the market. Each configuration of the system parts would then become a different vertical sector platform (eCommerce, Airport, but also Banking, Tourism etc).

The proper virtual identity system and platform in ARIES is defined through related technical specifications (D3.1 and D3.2), the face acquisition and liveness detection techniques (D3.3), the security enhancement of ID documents and their verification on mobile devices (D 3.4). Given the fact that it is a set of interconnected software and hardware components and protocols, we refer sometimes also to two main sub-systems consisting of:

- ARIES identity management supporting modules
- User mobile app

The first part of the system (supporting modules) is responsible to create Mobile IDs cryptographically and biometrically linked to original eDocuments with the highest level of assurance, providing the highest possible trust anchor on an eventual trust chain. From such base Mobile vID, citizens are empowered to use the second

sub-system (mobile app) to derive, manage and securely storage new virtual IDs with different levels of assurance (lower) and of privacy (higher), enabling them to optimize security and privacy according to their choice or preference. Another functionality on mobile app side is user-friendly biometric authentication, that extends state-of-the-art biometric template-protection methods. While authentication based on hardware token such as a smartphone or a smartcard is already available on the market today, ARIES extends the current functionality with further trust-increasing features, such as use of the biometric sensor or secure storage.

3.3 *Modules and components*

As mentioned before two sub-systems (identity management support modules and user app) are composed of many components and some of these may be deployed or used by a different stakeholder in the ecosystem. The module developed for biometrics capture, for example, ensures the functionality of document verification (such as National e-ID card or e-Passport) but it has client and server (service) side and can be deployed in two modes: local or packaged with online service by service provider. Generally speaking, mobile device components should be easily integrated to other service providers' applications to protect their access, and are being compatible with standard mobile operating systems (iOS and Android). There are components that could be exploited also separately, such as for example secure wallet that is also targeting any app developer.

A number of components, such as integration APIs, will be made open source and distributed under open source licenses, to facilitate a wide adoption of the project outcomes in the European ICT security, cloud and big data ecosystems, to maximize impact on the market, but also to improve sustainability since open source communities would contribute to its maintenance. As mentioned before, large number of ARIES software components can be grouped under the name "Identity Management (IdM) modules", although we reckon that IdM is a mix of technologies and business processes and there is no single end-to-end approach to identity management even within the single business domain and technology context. So called "chain of trust" is very fragile in multistakeholder environment where different eID process steps (enrollment, usage, management) are linked to different stakeholders. In a matter of fact, packaging will be discussed in the last year of the project and the results will be included in D5.2, the final version of this deliverable.

In what follows, we list main components and identify their individual value propositions from the technical perspective. In a latter chapter, strengths and weakness analysis will be performed based on these value propositions, actual achievements as well as comparison to the competitors. These issues will be continuously monitored also in the last year of the project to ensure that they do not lose relevance in spite of rapidly evolving market trends. We organise components into groups, from initial enrolment, through usage of vIDs, to managing those identities and integrating them with mobile services.

At the time of writing this document, the first demonstrator has been completed and four different processes have been tested with the corresponding components. These processes are:

- Authentication and identity proofing based on ICAO ePassport
- Authentication and identity proofing based on Spanish eID card
- Biometric enrolment and authentication
- Virtual identity issuance, derivation and authentication

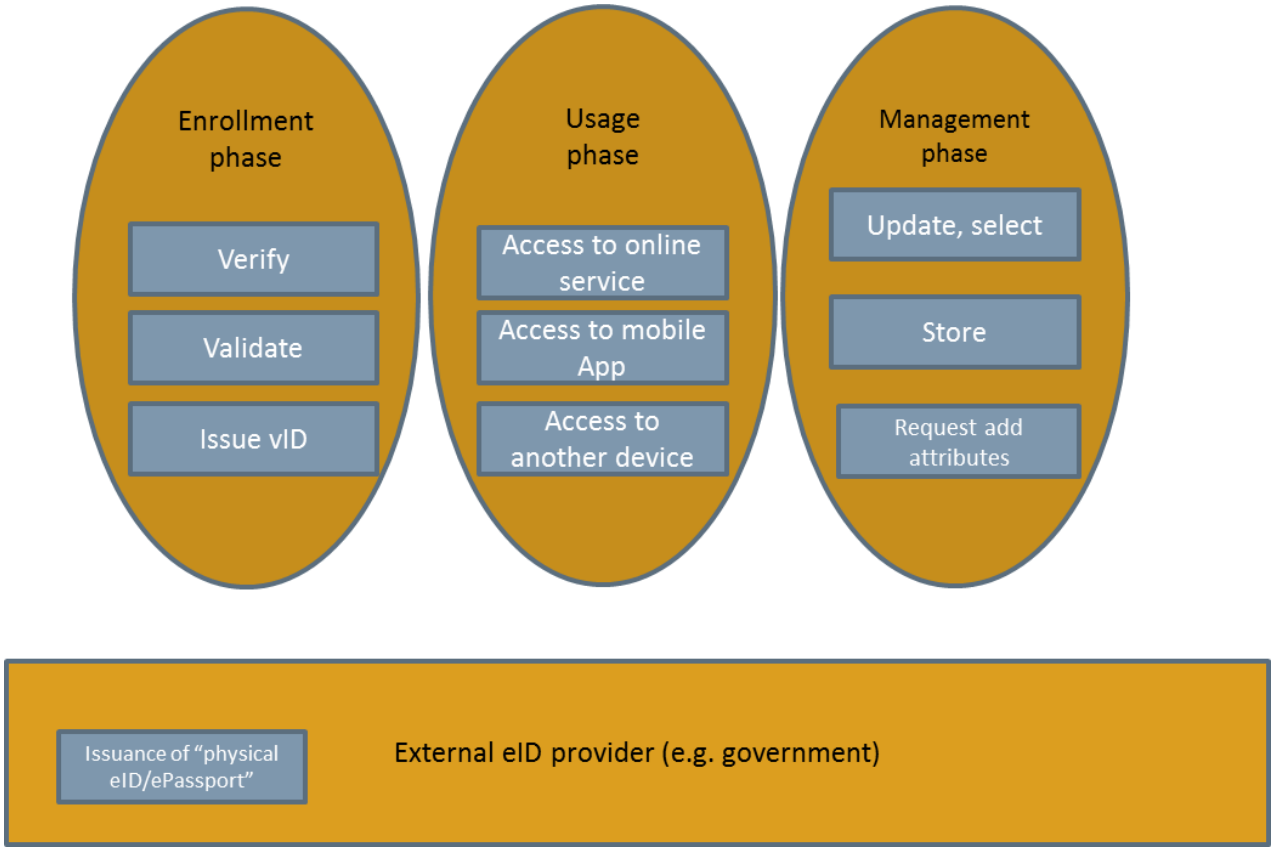


Figure 3: different phases of identity lifecycle

In the following subchapters we will give an overview of software components from the perspective of their applicability in different phases of identity lifecycle (see figure 3). However, we do not go into technical details related to the implementation, dependency on other components or integration options.

3.3.1 Enrolment components

Virtual identity enrolment includes a number of processes, such as issuance, based on process of derivation, as well as previous identity proofing and verification (IPV). It should be noted that IPV can consist of many checks, including online validity verification or checking blacklisting. In principle, citizens can enrol in the ARIES app through a number of steps:

- taking a selfie with an Android or Apple smartphone
- verifying their phone number
- taking a test to prove they are who they say they are

The selfie is the preferred option, linked via the app with a photo-ID document such as a driving licence or passport, while eID or ePassports document proofing adds layer of security. Verification of electronic data stored on eID card or ePassport is strong value proposition from ARIES, as opposed to many IPV solutions on the market.

A virtual identity is a central concept in ARIES and represents a subset of a citizen's identity, collection of the attributes, derived from the eID or ePassport, which should ensure disclosure of personal information proportional to what is needed by service provider. Citizen could for example create one vID for eCommerce purpose and a different one for check in and acquiring of the boarding pass. In some cases vID are referenced

by pseudonyms that cannot be linked together easily with the real identity (except when required by law enforcement).

The virtual identity derivation is a mechanism enabling users to create "companion" credentials cryptographically and biometrically linked to their source trusted documents, such as eID or ePassport. This includes methods of verifying the link between an electronic document holder and the identity contained in the document. ARIES is defining specific derivation mechanisms, including source document ownership verification techniques, and strong authentication means while preserving end user privacy. Derived credentials may include claim-based authentication capabilities, based on proof of credentials in a private way, giving users full control over their data to determine which private data is disclosed in each context. The main components for this phase of ARIES identity lifecycle are:

- Virtual Identity Issuer, which is server based component responsible for provisioning and management of main user Virtual ID. 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. 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. In case that Anonymous Credentials are used this module implements the Idemix Issuer role of the protocol.
- Issuance manager is a component that interacts with the Virtual Identity Issuer Service during the enrolment stage in order to obtain the vID. It is able to generate Mobile PKI key pairs, and send the CSR to the Issuer. In case of adopting Anonymous Credential systems, it would play the recipient role, to carry out the issuance protocol to obtain the crypto credential. In case Anonymous credentials are used, the Issuance manager can play the role of recipient in Idemix protocol.
- Biometric Mobile Enrolment components are responsible to register the user in the system. ARIES is including anti-spoofing solutions (i.e. live face detection) to prevent from fraud, including the definition of how to maintain privacy when using biometric verification, as well as the study of the legal and ethical impact of biometric verification. The main requirement was to ensure a good level of assurance while allowing self-registration on a smartphone. A mobile application manages digital and physical security checks of the eID: it captures a biometric feature of the subject, and while connected to a dedicated service, it also checks authenticity of the chip inside the eID (see proofing client and breeder doc verifier), consistency with the physical part of the document and the comparison of the biometric data with the reference biometric data in the chip will be verified. Thanks to the security features of the eID document and the additional use of anti-spoofing technology for biometric recognition, the process will provide high level of assurance.
- Proofing client collects evidences (chip data, and biometric data) and communicates with the ID Proofing Service to check authenticity of the data and consistency of the content. It basically validates that the user owns a recognized identity.

ID Security Features of eID card or ePassport are used to identify an original ID or eID Document, and they can be revealed by sight, touch, scanning or photocopying. ARIES is defining the verification of ID documents from mobile devices, combining visible end electronic domain security features. Examples of the proofing ID mechanisms that are being considered for the ARIES pilots are related to electronic security features of ICAO compliant eMRTD (i.e. ePassport) and the Spanish official eID card (electronic DNI). In so called Privacy-preserving virtual identity Proving, open source components are used, namely Anonymous Credential Systems (ACS), such as Idemix or U-Prove that allow users to present Zero Knowledge cryptographic proofs in order to prove possessing certain attributes in the credential. These systems enable a selective disclosure of identity attributes to achieve a privacy-preserving identity management approach. ARIES tries to introduce simple versions and adaptations of the Anonymous credential Systems concept, deriving different digital partial identities over the whole original credential obtained from the ARIES IdP.

3.3.2 Usage components

It is vital to distinguish between vID use in different contexts for different purposes. What may be ethically acceptable in security related circumstances (where 'exceptions' to legal requirements are important up to a point) may be unethical and deter societal acceptance in others. Online service providers might request lower identity assurance levels from vID, in exchange for wide user acceptance (such as the case of social logins). Finally, users themselves might have their preferences, for example related to privacy or identity attributes they want to disclose. Therefore we can talk about context-sensitive usage of vIDs, as one of the main value propositions.

The main use cases where mobile vID can be used are:

- Mobile device access to online service or access to sensitive data
- Physical access control, such as access to boarding zone in the airport
- Proximity or remote payments
- Access to another mobile app on the same device

In table 1 there are few examples of this usage mapped into the level of assurance expected from e-Id and in consequence also from vID.

Usage of mobile vID	Example Service	Level of Assurance
e-government license issuing	Fishing license	Substantial
Authentication to access sensitive data	Clinical records or financial data	High
Access buildings or restricted areas	School or university entrance	High
Mobile payments	Proximity combined with in-app payment	High

Table 1: mapping service provider risk

The main component related to usage of vID is authentication client. 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 authentication is done after the vID authentication. Authentication client also interacts with the vID Verification Service in order to authenticate the user. In case Anonymous credentials are used, this authentication client plays the role of prover in Idemix protocol.

vID verifier is responsible for verification of the ARIES vID, 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 Auth client module in the user smartphone. In addition, the vID Verifier service can verify derived partial virtual identities. In case that Anonymous Credentials are used this module implements the Idemix Verifier role of the protocol.

Breeder doc Verifier reads and verifies the breeder document through NFC technology. Interface between the documents (passport and Spanish eID) and the ARIES ecosystem. Biometric verifier does similar when the user biometric authentication is requested. It captures a fresh and live biometric image (with smartphone app) and execute the comparison with biometric reference collected during enrolment.

3.3.3 Management components

In principle, all phases of identity lifecycle, including enrolment or usage, are part of identity management. However, in this chapter we refer to this phase as "all other" components. The main reason for this is related to ARIES exploitation strategy, namely possibility to replace components (e.g. proprietary with open source) within a single identity lifecycle phases as well as to offer separated components (e.g. identity proofing and validation (IPV) as a separated offering, something to be discussed and described in D5.2.

Therefore in this section we include components related to maintenance and evolution of identity attributes, suspension or deletion, storage etc. More specifically we describe components developed in the project that enhance the existing management procedures and processes.

Credential manager and Identity selector is a component that manages the credentials stored in the wallet, forming Aries virtual IDs, and associated crypto material. It can communicate with the service provider to agree which particular attributes are needed to access to a particular service. It allows choosing the suitable partial identity that holds the minimum set of personal attributes according to the info required by the SP.

Secure Mobile Wallet is a component that stores cryptographic keys, pseudonyms, ARIES vIDs (tokens) and biometric data. In principle, it is a secure element in the mobile storing virtual identity, allowing to rigorously control its access according to pre-defined authorizations based on strong authentications. ARIES envisages defining a wallet with security functions ensuring data authenticity, integrity, non-repudiation, confidentiality, auditability and privacy. Including also protection against internal and external attacks. A secure electronic wallet will be provided to users for them to securely handle and manage their digital identities and their related data such as biometric information.

Finally, Secure Identity Vault is an important component for the inclusion of law enforcement authorities in the eID ecosystem since it stores evidence collected during enrolment (in particular from the proofing phase). It would offer basic Create, Read, Update, and Delete features. It is implemented as a secure space on the server storing confidential and sensitive information, allowing to rigorously control access according to pre-defined authorizations based on strong authentication and legal statute. Secure vault technology is not new by itself and several products on the market are able to provide integrity, confidentiality, auditability and compliance with various security standards and legal requirements; to ensure that the content is safely stored, non-repudiation is enforced, and its authenticity can be legally assessed.

3.4 *Packaging strategy*

While ARIES components are clearly identified and their intellectual property (IP) has been discussed and assigned unambiguously to the owners, the packaging strategy is still under discussion at the time of writing this deliverable. It is clear that many services are needed for the implementation of ARIES platform, from consulting through system integration to the support and maintenance. On the other side, purely architectural division of components, which was used for IP ownership assignation, might make no sense for the commercial offering, once that positioning has been clarified. In a matter of fact, early market study shows that IPV market (identity proofing and verification) might be the primary focus for ARIES, while target audience would depend on usage (identity provider or service provider). More details will be given in D5.2.

4 Business and stakeholder analysis

In Europe, identity ecosystem (we use it as a synonym to e-ID or digital identity ecosystem) is, as mentioned in chapter 3, often considered to refer to very large-scale identity management scheme, with its standards, protocols etc, as well as its stakeholders, from identity provider to identity owner. Most notable and relevant examples we have mentioned in chapter 3 would be eIDAS ecosystem, ICAO ecosystem and eCommerce ecosystems (in plural since there is more than one). Types of actors within the eIDAS identity ecosystem, for example, are diverse, although there are some specificities. Its focus is mainly on the cross-border recognition of so called "notified eID". This new concept is basically e-ID scheme notified by central government and can refer to "e-ID issued by the government, on behalf of government or under the control of government", therefore including both public (e.g. national e-ID card) and private (e.g. Bank e-IDs in Scandinavia) identity providers. The second specificity is in the architecture, where the central role is envisaged for "eIDAS node operator" (see figure 4), a stakeholder from the government that acts as a proxy to national identity providers. In ARIES the concepts that are used are derived credentials, virtual and mobile e-ID, which are linked to government issued physical ID, which can be eID (here is the overlap with eIDAS ecosystem, since all eIDs in Europe based on national eID card will become "notified eID").

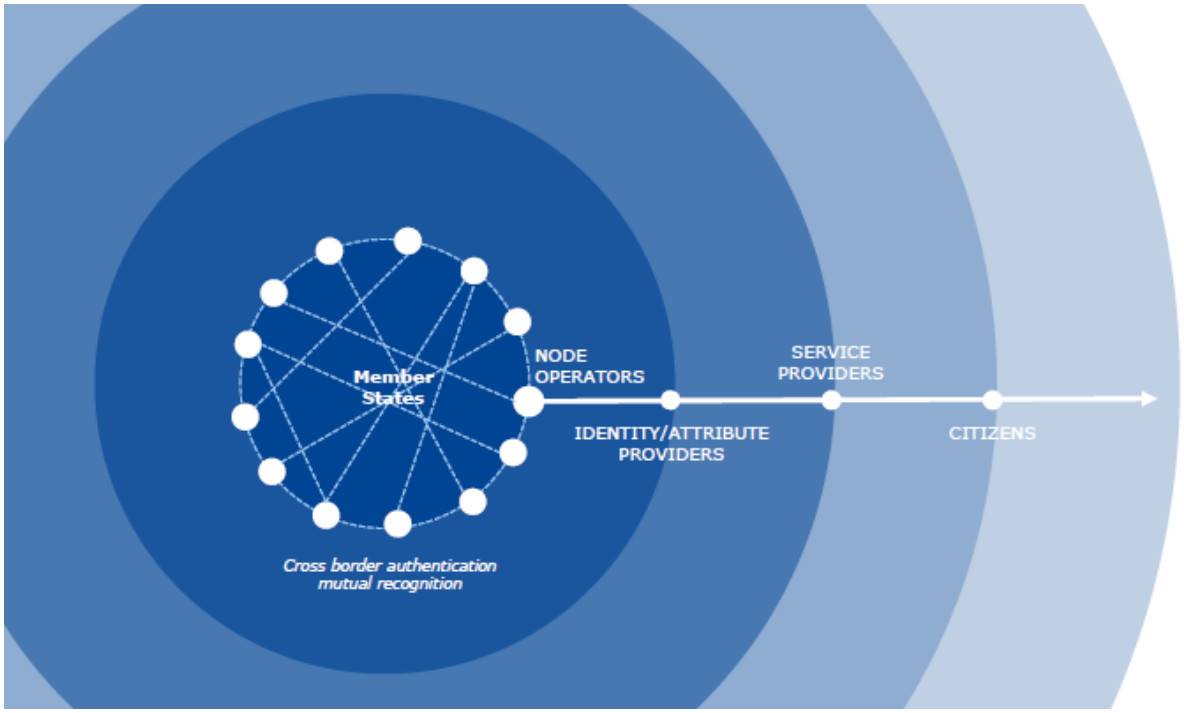


Figure 4: eID ecosystem example - eID under eIDAS compliance

The other document ARIES can use as a "breeder" document is ePassport and for the e-ID ecosystem around ePassport we use term "ICAO ecosystem". International Civil Aviation Organization (ICAO) is United National organization that standardizes passports worldwide. Similar to e-ID card, ePassport certifies the identity of its holder, but the primarily purpose is international travel. There are over 120 countries (as of 2017) that have obligatory biometric information in a microchip embedded in the e-Passports.
A number of countries, such as Andorra, Australia, Canada, Denmark, Japan, New Zealand, or United Kingdom does not have national identity cards, so ePassport would be the only manner for them to use ARIES.
ICAO is distinct from other international air transport organizations, like the International Air Transport Association (IATA), a trade association representing airlines that can considered as another important

stakeholder in “ICAO ecosystem”. In Europe, in a package of initiatives on security, the European Commission proposed, in April 2018, improving the security elements of EU citizens' identity cards, so it is expected that e-ID card and ePassport ecosystems will become closer in the future. ARIES could be an important “bridge” between physical and virtual uses of these identity documents.

The third relevant ecosystem relevant for ARIES is more complex. We call it “eCommerce ecosystem”, but since each eCommerce service provider has several options, including operating its own identity management, we talk about several “flavors”. We will limit our attention to the use of e- IDs, such as social network login, for the access to online services such as eCommerce. Since these e-IDs do not necessarily match one to one to a physical identity, we can consider them also as a kind of vID (although low assurance, as compared to ARIES vID).

While analyzing future ARIES ecosystem, roles and responsibilities, we will look at the current situation and trends and will try to answer questions such as:

- Are current eID or ePassport identity providers likely to become virtual identity provider?
- Is a biometric verification provider necessarily the same as a virtual identity provider?
- Who operates secure vault in ARIES system and who decided on the cross-border access control for LEA?
- What is the role and responsibility of external stakeholders, such as attribute providers or mobile operators, in the ARIES ecosystem?

In order to analyze this and other questions we also look at identity lifecycle management, or ILM. ILM encompasses the collection of technologies and business processes utilized in creating, managing, coordinating and restricting the e-identification, as well as access control, and governance steps or issues related eID. Secure enrolments, for example, are increasingly important part of identity management and the current practice of face-to-face verification, which is required for high assurance level of identity, is not cost-effective, which results in a market trend to separate phase of secure enrolment (digital on boarding) from the other phases and sell it as a separate service. In recent years there are several attempts to launch schemes based on remote self-enrolment of users where, of course, security requirements remain strong, but are harder to guarantee.

The idea of the ARIES value chain, on the other hand, is based on the process view of different stakeholders, with each stakeholder being part of overall e-ID ecosystem, made up of technical subsystems each with inputs, transformation processes and outputs, that might or might not coincide with identity lifecycle steps.

In ARIES ecosystem each stakeholder has its own role and motivations, its expected costs and benefits, drivers and constraints. In deliverable D2.3 stakeholder analysis was done from both functional and legal perspective, while D3.1 has more technical and process-oriented description of required capabilities and capacities.

The result of this analysis has also to be fed back to the positioning and packaging strategy (to be described in the next deliverable D5.2) where components have clear relation regarding the each roles identified, such as virtual identity provider (IdP), Service Provider, User/Citizens, Law Enforcement (inspector), as well as external stakeholders such as Attribute Providers or Certification Authority. In theory, services provided by IDM sub-system components can be offered by different stakeholders, but additional requirements such as trust enablement, must be taken into account. Mobile app that is downloaded by citizen needs to incorporate the corresponding libraries to interoperate within the proper IdM service being adopted and customised by specific IdP. The integration with secure vault that stores the correlations between the different virtual IDs or pseudonyms that user holds, and is used for auditing the process, is another customisation issue where additional stakeholders might be involved (e.g. secure vault can be part of a larger cloud infrastructure operated by public administration).

Service Provider (SP), also called Relying Party in some identity frameworks, provides one or several web or mobile applications that offer their services and in turn rely on the vID Verifier service for authentication. The SP might require specific attributes that will be needed to permit the user access to his service. User needs to give consent prior to sharing the partial vID holding the required attributes. The SP might also be able to verify by himself the partial vIDs without relying on the external IdM vID verification services.

This verification model increases the complexity and burdens the interoperability in the SP but, at the same time, increases the unlikability and reduces traceability against the IdM services.

Verification of vID can be done by a virtual vID provider (or called simply IdP) or directly by SP, but 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.

This means that besides acting as vID provider (VIDP) an existing identity provider (IdP) can also take role of biometric verification provider (BVP). It is ONLY used for high assurance cases and IF 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.

Given that the ARIES ecosystem architecture allows different roles to be assumed by different providers, an appropriate liability regime must be established between them, through the corresponding contracts, since the final responsibility lies with the provider that issues the derived identity; that is, the corresponding electronic identification mean.

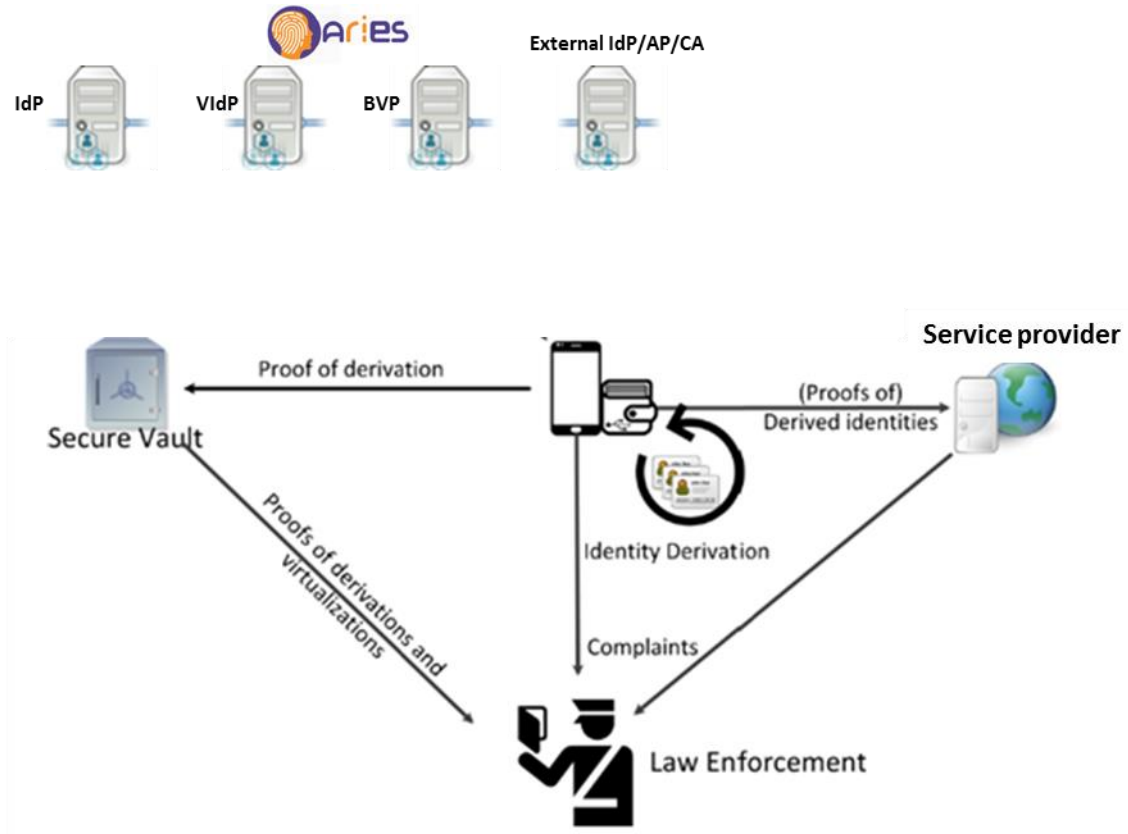


Figure 5: stakeholder in ARIES ecosystem

Especial attention has to be given to the role and responsibility of Law Enforcement Authority which is in charge of the inspection of the transaction logs stored in the vault when the conditions for inspection are met. It performs sort of de-anonymization of the user and audits log data related to vID usage stored in the ARIES Security Vault in order to prevent or investigate identity fraud, misuse, liability or cybercrime. Specific policy that describes which information should be recoverable as well as the circumstances under which the data can be inspected is subject of other deliverables. This authorization privilege is providing LEAs with specific cryptographic credentials that allow decryption of such information.

In ARIES ecosystem (see figure 5) we sometimes refer to ARIES IdP as an single operator of different services, such as vID issuance and management or biometric enrolment and verification while other stakeholders, such as law enforcement authority (LEA) or even mobile operator (see deliverable D3.1), are included. Since creation and management of virtual identities contemplates possible aggregation of authentication credentials and attributes from different external identity or attribute providers, we can also envisage role of intermediary between SPs and end user information stored in authentication and attribute providers.

ARIES role	Examples	ID management functions to perform
End user	Buyer, bank customer, traveler, etc.	Authentication, in some cases self-enrolment
Trusted document issuer	National ID agency, passport agency	Provision of "breeder" document for verification
Virtual ID provider	Mobile network operator, banks, utilities, healthcare providers, online commerce platforms, aviation, etc.	From enrollment and issuance to storage
Enabling and Support	Regulatory agencies, standardization bodies, trust frameworks, etc.	Audit, support

Table 2: Roles and examples of target audience

Besides attribute providers, other external stakeholders have important role in ARIES ecosystem (see table 2). When it comes to enabling and support roles, it is important to address issues such as who will take responsibility for reparations in the event of negligence, or who will have an audit role. In case of identity federations or cross-national schemes and ecosystems such as eIDAS, we can also think of additional roles, for example who will take care of matching and mapping national levels of assurance (LoA) into the eIDAS defined levels.

In ARIES there is a reliance on the e-ID card or ePassport issued by the government. In some members states e-ID card does not exist or doesn't have an NFC readable chip, so we might distinguish other cases of "alignment with eIDAS ecosystem":

- eID directly issued by the government, but not in a form of e-ID card: this is the case of "login type" of e-ID (see figure 6)
- eID issued on behalf of government, derived from government identity "root" eID or issued under the responsibility of the government, such as Bank ID (see figure 6)

It is clear that different strategies will have to be pursued in different countries, and that verification of national e-ID card will not be service of interest for some markets.

A different situation occurs with ePassports, used in ARIES as breeder document. For ICAO, that issues standards related to ePassports, breeder document is considered to be birth certificate or similar. ePassports, unlike e-ID cards, are currently not used for online business.

Country	Name of the eID scheme	Type	Status
Austria	National Citizen ID	Multimean	In use
Belgium	National ID	Smartcard	In use
Bulgaria	National ID	Smartcard	In development
Croatia	e-Citizen	Multimean	In use
Cyprus	ARIADNI	Login	In use
	National ID	TBC	In development
Czech Republic	National ID	Smartcard	In development
	mojeID	Login	In use
Denmark	NemID	Login	In use
Estonia	National ID	Multimean	In use
Finland	FINeID	Certificates	In use
	TUPAS	Mobile	In use
France	FranceConnect	Login	In development
Germany	National ID	Smartcard	In use
Greece	ERMIS portal	Login	In use
	National ID	Smartcard	In development
Hungary	eSzemelyi	Smartcard	In use
Ireland	MyGovID	Login	In use
Italy	SPID	Multimean	In use
	National ID	Smartcard	In development
Latvia	eParaksts	Smartcard	In use
Lithuania	National ID	Smartcard	In use
Luxembourg	National ID	Smartcard	In use
	LuxTrust	Multimean	In use
Malta	National eID	Smartcard	In use
Netherlands	DigID	Login	In use
	eHerkenning	Login	In use
	Federation: Idensys, iDIN, DigID	Multimean	In development
Poland	National ID	Smartcard	In development
Portugal	Cartão do Cidadão	Smartcard	In use
	Chave Móvel Digital	Mobile	In use
Romania	National ID	Smartcard	In development
Slovakia	National ID	Smartcard	In use
Slovenia	eUprava	Certificates	In use
Spain	National ID	Smartcard	In use
	Various*	Certificates	In use
	Cl@ve	Login	In use
Sweden	Bank ID	Multimean	In use
	e-Legitimation (Telia)	Multimean	In use
United Kingdom	GOV.UK VERIFY	Multimean	In use

Figure 6: Status of national e-ID schemes likely to become "notified e-ID" in eIDAS ecosystem

In an extended ARIES ecosystem there is also a role of Attribute Provider (AP) as a source of user attributes. While some attributes are acquired from eID/ePassport during enrolment process and stored in user Secure Wallet, the other could be acquired from the external sources or direct input from users.

Another external stakeholder is certification authority (CA). In initial stages of the project the user credentials were based on pseudonymous PKI scheme. The Certification Authority is responsible:

- Authentication and authorization of parties requesting new certificates
- Generate pseudonymous certificates
- Maintain certification revocation list for enrolled vID credentials
- Optionally maintain list of trusted certificates or trusted service list for document verification (ICAO or eIDAS).

In the figure 5 we include service provider (or relying party, as it is called in some ecosystems) as an integral part of ARIES ecosystem. However, Service Provider (SP) has also variations, depending on the use cases proposed by the ARIES platform prototypes:

- online authentication to a web service, applied to eCommerce use case
- face to face ID verification and access control, applied to Smart Airport use case

In both cases, additional external stakeholders can be needed on service provider side, e.g. mapping or translation of protocols (identity broker) or customisation services. Some external IdPs that provide additional

certified attributes, not extracted from e-ID or ePassports, are not necessarily aware of ARIES technology, but could be contacted by the vID Verification service in order to authenticate the user through other protocols-technologies. In any case, the usage of these external IdP would require that the user, the SP and the vID Verification service trust this external IdP. In some cases, only one or more attribute is requested from these external IdP, which reduces these stakeholder to the role of Attribute Provider previously described.

4.1 *Target audience and main messages*

The majority of existing solutions are not suitable for the market needs because there is a lack of solutions, including consistently applied technologies and processes for trusted enrolment, identification and authentication processes, in particular considering the widespread the use of online credentials with low levels of authentication assurance.

The main aim of ARIES is to bridge this gap through a European electronic identity ecosystem capable of addressing the challenges posed by wrong identity, identity fraud and associated types of cyber and other forms of organized crime.

A subset of stakeholders described in the previous chapter is ARIES exploitation target audience. These are stakeholders that will pay for either ARIES project results or services and will be also the main target for the dissemination activities and in particular associated partnership. Continuous market monitoring in order to detect new trends and possibilities, which will allow the consortium to react to the market changes and adapt the implementation of the new versions of ARIES components will further shape ecosystem and will fine-tune both business models, as well as target audience messages.

e-ID market is so called multi-sided market where higher number of service providers offering specific eID scheme is influencing increase of citizen eID adoption and use, and the other way round: the more eIDs is issued by eID scheme and used by citizens, the more likely is that service providers will be interested to adopt it for authentication and other services.

Taking a social perspective based on Diffusion of Innovations theory[2] we might propose different strategies to adopt innovations more successively. The first group, the innovators, make up merely 2.5% of the population that wants to try out the ARIES innovations even before there is a full ecosystem. These are pioneers that we target with ARIES associated partner group. These early adopters need to find value in using the platform and to convince more people to join the ecosystem. The key seems to be to start within a niche (e.g. ARIES platform for Smart Airports) and with a specific purpose, deliver stand-alone value, such as saving time regarding face to face verification, within the targeted subgroup.

From a practical standpoint, the target group could be any stakeholder interested in bridging digital and traditional approaches (i.e. physical and electronic identity documents, virtual identities) in order to increase and sustain high technical and procedural levels of quality of security documents and corresponding processes in both virtual and physical worlds. This could include hotel chains, rent-a-car companies, banking organisations that must comply with anti-money laundering directive (AML4) and others.

From a policy perspective, the issue is not so much in who is the target audience (clearly it is European Commission), but what is the message to bring. Cross-border recognition of electronic identification means under eIDAS regulation is opening many possibilities. One is that virtual IdP, such as the one envisaged in the previous section, is considered as a service provider in “eIDAS ecosystem”. The second possibility is elevating the service offered by the ARIES v-ID provider as new electronic identification service under eIDAS themselves, meaning that the partial, derived identity is considered as a specific type of “notified eID”, recognised under the eIDAS rules.

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

Even more, probably the most relevant policy contribution is the possibility of characterizing the service offered by the ARIES provider as a new trust service: the accreditation of possession of personal attributes (a wide conceptualization of identity) with privacy protection. An ARIES provider, once a person identity has been provisioned, offers a service that allows that person to self-create partial, derived, identities asserting in a trustworthy manner a particular personal attribute (i.e. the possession of a personal, valid, boarding pass to shop in the airport, or being older that certain age…). These derived identities have to be considered assertions that may legally substitute in some scenarios the corresponding documents that evidence the personal attributes (i.e. instead of showing the boarding pass, with all personal data, one shows a partial, derived identity that proves the fact that the person has a personal and valid boarding pass); thus increasing privacy effectively while reducing compliance costs to data controllers.

5 Market analysis

All over the world national e-ID schemes, as well as mobile eID, increase in number, visibility and reach. Smart borders/smart airports also emerge at a faster pace, while eCommerce is having spectacular growth, although mainly thanks to the centralised marketplaces, such as Amazon or Alibaba. Today there are 700 million plus ePassports in circulation, while the number of electronic National ID cards in circulation will reach 3.6 billion citizens by 2021, according to research company Acuity Market Intelligence (March 2017). Early 2017, 82% of all countries issuing National ID cards have implemented eID programs, with a strong push for biometrics. All these facts create a strong momentum for ARIES adoption. It seems that the right opportunities exist both at the demand side (identity providers, service providers, citizens) and on supply side (technology providers).

In line with the previous stakeholder analysis, in preparation for market and technology analysis, we did alignment and mapping between:

- Demand-side objectives and priorities: in multi-sided market we have several stakeholders on demand side: citizens, but also service providers. Their objectives might differ, for example SP will yield for greater effectiveness (better security, higher assurance level…), efficiency (faster or cheaper authentication, sharing of additional attributes, etc) and transformation (use of mobile phones as sales channel, opening to cross-border business etc). On the other side, citizens objective might have conflict with some of these goals. Privacy preservation, for example, might be desired by the customer, but it impedes personalized targeted marketing from the online service provider. We will use some lessons from the past in order to pick up the best practices in balancing interest of different stakeholders.
- Supply side analysis: these are products or services that might be considered either competitors, alternatives or complementary to ARIES assets. Here we look more at underlying technology or components that the adoption trends. ARIES components are already described in other deliverables with several references to underlying technologies, tools, techniques, etc that are also collected and presented here.
- Challenges and trends: these are analyzed in parallel for demand and supply side. While the use of digital online identities with low level of assurance is rather common today (especially OpenID based schemes) we look at the challenges and trends related to elevation of level of assurance for e-ID, including virtual IDs. We also look at market analysists reports and reflect so called “hypes” in digital identity business. Sometimes, different names are used for the same market trends or technology building blocks, but the main focus in this chapter will not be on comparative assessment.

The main input therefore for shaping business based on ARIES, will be from demand-side, but given the low responsiveness and predictions focused too much on the “short term”, we will also involve external consultants or market analysts, some of which are represented in ARIES special interest group. The idea is to look at more mid to long term evolution of demand side needs and to define situation “*to be*” as well as transition from “*as is*” scenario (GAP Analysis).

Policy analysis is excluded from this chapter since it has been described in D2.2. However, since many conclusions of this deliverables have direct impact on SWOT analysis (e.g. namely opportunities related to eIDAS entry in force), we will repeat or summarize some conclusions from it. The immediate context for ARIES is expanding use of biometric tokens in line with the recent proposal of EC to strengthen the security of ID cards. Since biometric eIDs originated in border management scenarios, immediate context and usage scenarios cannot be directly translated into the online “consumer” services such as eCommerce. On the other hand, recent cybersecurity directive (sometimes referred as NIS directive) is directly targeting “market

operators" among which online service providers are especially vulnerable. Virtual low assurance ID, such as pseudonyms, originated in this world, so ARIES is somehow placed at the border between two worlds that have different market and policy background that now need to come closer in order to combat fraud and ID theft, whether it is border control or daily use of online services by the citizen. With the increasing convergence of physical and virtual worlds (think of Smart Cities, Industry 4.0 etc), our physical and virtual identities need stronger and more traceable links. Thanks to the advances in technology and business model innovations in ARIES, this is now possible to achieve with the adequate level of privacy preservation.

5.1 *Demand side analysis*

Various efforts have been made up to date to create, issue or manage multiple variants of electronic identities. Demand from citizens resulted in growth of usability and user-friendly features, such as cross-domain single sign on (SSO), meaning that citizen can authenticate once and then gain access to protected resources in a variety of places, without being asked to re-authenticate. On the other side of the demand, service providers were requesting innovative solutions for increase of strength or share of attributes. In parallel, divergence of technical options on supply side, e.g. use of tokens, smart cards and more recently mobile phones, resulted in a complex and fragmented market that sometimes can result confusing to the outsiders.

It has been widely acknowledged that the societal acceptance of eIDs may be compromised by the inappropriate use, potential loss, misuse or impersonation of an individual or cluster of individuals whose data has been fraudulently acquired. Recent years also witness a real tsunami of cyber-threats related to identity, including to the use of **biometric technologies.** As an alternative to a PIN, the biometrics capability is becoming featured in many smartphones, especially as the second authentication factor. Biometric authentication also enables user to log in anonymously without sharing any data with the website or app.

Europe is forerunner when it comes to the use of biometrics, notably fingerprint and facial image scans, for official documents on smart cards, but is also leading the research in **privacy preserving identity schemes**. Combining these two areas in a single project and a single ecosystem is the main added value of ARIES. It is a complex project and the success will not be easy to achieve. However, even the putting the first bricks for the bridge that will cross two worlds, one of high level of assurance of identity, and another one of citizen preferences regarding privacy, is already an important achievement.

Attitude towards online privacy and actual behaviours of citizens is sometimes not clear or at least not valued correctly. While in airport context, for example, citizens are giving up their privacy without discussions, in online service context there seems, at least in many cases researched by Alessandro Acquisti [3] , to be divergence between what people say and what people do, in regard to the value of privacy. This behaviour is often explained by "networking effect" of multi-sided markets, by "freemium behavioural economics" or simply by the lack of awareness. The lack of motivation for service providers to adopt privacy preserving mechanisms could be another possible reason, that we have less and less privacy online. This motivation can come either from legal obligations (e.g. compliance with regulations) or from market logic (e.g. users preference for privacy preserving e-ID). This existing "take it or leave it" approach in predominated situation regarding the online e-ID services, however, is set to change with the increased awareness, availability of privacy-aware identity schemes, and entry in force of **general data protection regulation (GDPR)**. In addition, it can be expected that businesses that implements high standards of privacy, proportional to the risk they have, may enjoy higher levels of public trust in their products or services and therefore have competitive advantages. Proper balancing when it comes to privacy and security, therefore, becomes an important part of the adoption model as well as a part of decision making in digital ecosystem.

The regulatory landscape is not limited to GDPR. We have already mentioned eIDAS which mandates to establish three Levels of Assurance - LoA (in some government guides, like UK, these are called "assured identity levels") , which categorize the notified eID schemes according to their security, covering the complete lifecycle of the credentials, including enrolment, issuance of the credentials, usage and finally revocation. The Expert Group beyond this decision decided to go with an »outcome based approach«, i.e. not requiring concrete technology to fulfil security goals, but stating the fulfilment of a security goal itself as the requirement

for LoA. In some member states it will be challenge to map levels into LoA and to match solutions from different MS into these three levels. Other regulations that will have an impact on service provider adoption of e-ID technologies are the fourth anti-money laundering directive (AML4), with the requirements related to know-your customer (KYC), as well as the second payment service directive (PSD2) that introduces concept of Strong Customer Authentication (SCA). The rest of this chapter looks closer to these demand side trends, starting from the existing and future eID ecosystems.

5.1.1 Evolution of identity ecosystems

In chapter 3.1 we have already defined what we understand as "identity ecosystem" and in chapter 4 we have analysed role and responsibilities of the main stakeholders in it, with special focus on what we denominated "eIDAS", "ICAO" and "eCommecre" identity ecosystems.

In the figure 7 we present another perspective of eID ecosystems, this time having in mind its architectural and governance characteristics. As mentioned before, official government issued identity documents (e-ID cards) are expected to be predominant types of e-ID schemes recognized as "notified ID" in eIDAS jargon and could be directly for services such as cross-border online service authentication. This type of solution is seen as "strongly centralized" ecosystem, with a central government being responsible for most of identity lifecycle phases, from breeder documents (such as birth registry) issuance, e-ID issuance, identity proofing and verification, to the enablement of authentication through government operated national eIDAS nodes.

Figure 7: different types of identity ecosystems

The second type of national eID schemes (that are likely to be notified and form part of a future eIDAS ecosystem) is exemplified by the Nordic countries e-ID, such as Norwegian or Swedish e-ID. Government operates a national register of personal ID numbers which constitutes the base to every public service as well as many private ones. Nordic countries are having ID cards being issued and distributed by private

organizations, mainly banks and post offices, containing this government issued personal identification number. Therefore we talk about government-licensed or government endorsed e-ID where banks provide the user base and the government regulates by legislation and requirements in recurring procurements and "framework contracts" (today there four contracted providers in Sweden, for example). There is still "central" element in eID ecosystem, namely Tax Authority which handles procurement, administration, and operation of population register. eID is not necessarily issued on smart card. There are versions of soft eIDs, a file downloadable to the user's compute, as well as "hard" which comes on a smart card, sometimes targeting different audience or different purpose. For example, the soft eID is today used for online transactions, while cards such as Swedish NIDEL ("National ID card prepared for E-Legitimation"), issued by the Police, is motivated by other arguments, such as identification needs of the Schengen Treaty. This separation of "breeder document" issuance and management and eID issuance and management can be easily extrapolated to ARIES situation where the existing e-ID cards become "breeder document" and vID becomes what is e-ID in Nordic countries – operated by several different vID providers.

Norwegian BankID is a personal identification issued by the banks in Norway, based on a coordinated infrastructure developed by the banks under the direction of the "Finansnæringens Hovedorganisasjon" and "Sparebankforeningen". In the middle of March 2015 it was issued person certificates (PersonBankID) to more than 3.5 mill different persons in Norway. The total number of BankID-transactions in Norway is between 0,9 and 1,0 mill each day. Work on developing BankID as a joint infrastructure started in 2000, and the first customers got BankID in 2004. In 2014, BankID Norway AS was established. The company owns the brand BankID and is responsible for operation, development, communications and sales to user sites. More than 300 user sites in a number of different sectors offer login using BankID and BankID on mobile. Today, 3.7 million Norwegians have a BankID, and more than 1.000,000 have BankID on mobile. Electronic identity cards in Sweden are also called BankID, but it is different technology owned by different companies). As mentioned before, the Swedish BankID may be soft or hard, in the form of a certificate file on disk, on card, but also on smartphone or tablet. The latter trend (Swedish mobile BankID service) does not require a specific fee to the mobile network operator, and can be used both for authentication within apps and web services on the same phone, and web pages and services on other devices. It also supports fingerprint authentication on compatible iOS and Android devices.

In Switzerland an important step was taken towards end of 2017. Role of the state, namely Federal Council is limited to certification and monitoring the e-ID system and in addition to define and verify official identities. Private sector providers, however, will act as identity providers. Swiss Post, SBB, Swisscom, UBS, Credit Suisse, Raiffeisen, Zürcher Kantonalbank, financial services provider SIX and Schweizerische Mobiliar have signed a memorandum of understanding to establish a joint company that will create and implement a digital ID. This company, SwissSign Group AG, will integrate the activities of existing firm SwissSign AG from January 2018, and continue to develop the "SwissID" solution for citizens.

Joint ventures and public-private partnerships are also hot topic in Germany. Veridos GmbH was established in 2015 as a joint venture between two of Germany's best known providers of secure government solutions, Bundesdruckerei GmbH and Giesecke+Devrient GmbH. The Verimi GmbH (combination of words verify and me) is trying to take opportunity brought by GDPR and eIDAS as well as to match user centric identity management and privacy preferences. Verimi was founded in May 2017, supported by a broad alliance of international companies and sees itself as European answer to the big American and Chinese platform providers. Partners include Allianz, Axel Springer, Bundesdruckerei, Core, Daimler, Deutsche Bank with Postbank, Deutsche Telekom, Here Technologies as well as Lufthansa. The launch is scheduled for spring 2018, but in the meantime more partners, such as Giesecke+Devrient, have signed the joint venture contracts.

The third type of e-ID schemes is also national scheme, this time from UK, which introduces even further degree of decentralization and open market perspective. UK's Government Digital service (GDS) launched the UK Identity Assurance Programme under the name "GOV.UK Verify". It is roughly based on the system previously known as the Identity Assurance Programme (IDAP). Its main characteristic is that it is based on public-private partnerships. Unlike Nordic Bank ID that works with procurement and framework contracts, it is based on a federated identity scheme that leverages multiple distinct identity management systems. In UK

there is no government issued ID card, so identity verification is done through verification of documents such as passport or driving license and it normally takes between 5 and 15 minutes to verify identity the first time. In this type of e-ID ecosystem the opportunity for ARIES lies in this specific phase of e-ID proofing and verification, which is now mainly done through specific operator that connects to different databases. The confidence of an individual's identity is organised around four different levels with level four that requires confirmation, using biometrics, similar to ARIES. Most e-government services, however, require level two of authentication assurance. GOV.UK Verify works with Open Identity Exchange UK (OIX UK) and uses a kind of "hub" or marketplace that allows identity providers to authenticate identities without the government centrally storing an individual's data. Work is underway to extend usage of the system to the private sector, although there are some criticism around the system. The success rate in verifying individuals is 50% as of Feb 2018 (https://www.gov.uk/performance/govuk-verify/certificate-company-completion-rate) while some identity provider are removed from the list, such as Verizon. Thanks to excellent dashboard it is easy to track usage of e-ID (https://www.gov.uk/performance/services)

Finally, the last type of e-ID scheme in figure 7 is already mentioned "social network login". Although these e-ID are traditionally based on self-enrollment and have low level of assurance, more recently there is a trend to link them to government issued credentials, including e-ID card, passports (or driving licences). Facebook for example bough Confirm in January 2018, which is a software firm that specializes in authenticating government-issued identification cards. WeChat, the popular Chinese mobile application from Tencent Holdings, is also experimenting with virtual ID card, which serves the same purpose as the traditional state-issued ID cards. Tencent has estimated that the app reached 980 million monthly users at the end of September 2018, as WeChat team co-developed the new ID program alongside the Ministry of Public Security. In regard to this group of identity providers, ARIES offering might be limited to identity proofing and verification phase and its link to the already existing e-ID infrastructure.

Decentralized identity model has been there for many years, under different names (e.g. user-centric eID, identity 2.0 etc). While the idea to enable users to manage their own identity and profile attributes, technical implementations differ and more recently blockchain technology is used. While the previous solutions focused much on privacy, new generation based on blockchain technology is also addressing risk issues by balancing the accountability and responsibility of digital identity management across the value chain participants. A hybrid approach that combines advantages of centralised and decentralised schemes is now emerging as the optimal compromise, especially in B2C and B2B scenarios that manage sensitive or identity data. So called "identity trust fabric" is another hype term that refers to sharing of identity assets across people and organizations, based on blockchain platforms run by groups of organizations operating in trusted network, such as B2B ecosystem. The level of trust in these systems, however, highly depends on the quality of distributed consensus algorithms, as well as performance, efficiency and the probabilistic properties of it (e.g. hashgraph approaches are still in research).

In recent days, many blockchain-based ID solutions appeared like WorldCitizenship, OneName or ShoCard. They all use a decentralized approach by managing IDs on a hash chain and some of them market themselves as "self-sovereign identity" (see section 5.1.4 as well). A downside is that if the smart phone gets lost, there is no way for recovering one person's identity. Furthermore, potentially unqualified persons can create entries on the blockchain which leads to less trust in provided identities. On the other hand, no central node is needed to perform authentication between two parties. ShoCard is an example of a virtual identity card used through a simple mobile app. It has strong security techniques like multi key encryption in hashing, two-factor authentication, out-of-band communication and data matching. In their interviews authors have said it's built on a public blockchain data layer so as a company ShoCard is not storing any data or keys that could be compromised.

Besides direct integration of external social network e-ID services through the identity provider available APIs, e-service providers have also an option to use broker or aggregator of different identity providers that might offer additional functionalities, such as proxy to mobile devices, protection of consumer privacy and processing some data. One example is Gigya which has been recently bought by SAP. Other competitors include LoginRadius, Microsoft Azure AD, Janrain, Ping, Social Annex, Addshoppers, Ubisecure, Okta or OneAll. These

solutions are sometimes called Identity clouds or CIAM (customer identity and access management) solutions. CIAM claims many measurable benefits and return on investment, such as 20-30% more efficient marketing & sales, reduction of the abandonment rate during the registration (that can be as high as 70%), or savings through simplified and unified infrastructure. The business model of CIAM vendors is based on charge per user or per transaction and implementation usually takes from 4 to 6 weeks. For e-service provider there is no large investment since identity is provided from the cloud and support is given by CIAM operators.

5.1.2 Going mobile

Mobile ID solutions may be divided into two groups: shared secret based systems or systems based on centralized Public Key Infrastructure.

The shared secret systems are usually based on plain OTP generation [RFC2289] or challenge based OTP: OCRA [RFC6387]. The systems leverage on fact that same backend systems may be delivered for both physical device and App based OTP tokens, the former ones used mainly for high risk transactions. The App OTP tokens are usually used in two modes: the OTP may be displayed to the user and manually entered during the authentication or requested by push message (out-of-band). The OTP generator is usually protected by PIN or pattern, protection by biometry has been introduced quite recently. The OTP based mobile solution has an advantage of being able to work even when the handset is offline which was until recently considered important differentiator, because network connection was not available 24/7.

The Public Key Mobile ID ecosystems are usually based on similar to centralized PKIublic Key Infrastructure-based scheme and differ in the way the identity data is stored such as:

- SIM-based mobile ID: Data is physically stored on the SIM card of the mobile device. In some countries e-ID card is used as SIM card (Estonia, Moldavia).
- Embedded element mobile ID: Relevant identification data is stored in the embedded secure element (SE) of the mobile phone. Most governments still have concerns about data privacy when it comes to storage of government issued eID not entirely under their control. Storing the government issued electronic identity in a USIM, microSD or SE, therefore appears to be unacceptable to most governments.
- Mobile app stored ID: In 2017, e-ID ecosystem in Estonia was changed once again with the introduction of Smart-ID [14] , which is basically mobile application not connected to a physical chip. Before starting to use the system, users are enrolled and identity has been verified through other means (chip based ID or face to face by a teller in bank). Afterwards, two PIN codes are used (one for log in and another for transaction confirmations).This solution already has almost 500.000 users which can be considered as a success for a small country like Estonia. Similar approach is followed by the evolution of Austrian mobile ID, which is now called MIA [15] .

We can also differentiate mobile IDs in respect to the way identity data is generated or transferred to the mobile phone:

- NFC-based mobile ID: This solution uses the contactless NFC interface of the mobile device to securely access identity and authentication information from an external e-ID card. This is the case of Spanish eDNI card which is also used for ARIES pilots. Key requirements for contactless smart card readers reading contactless government eID cards are the greater field strength required from the reader to power the card, and that the reader might need to support extended length ADPUs to transfer longer pieces of data. At the moment the field strength issue seems to be less of a problem for NFC mobile devices then the “extended length” problem because extended length APDUs are not supported by the majority of smart phones today, although this is changing. The user identity may be based solely on the NFC document used, in this case any mobile handset may be used for authentication, or in associated mode when the handset is pinned to the particular user and works as an additional authentication factor. The NFC based mobile ID suffers usually from bad user experience: for some handsets it is hard to locate the NFC antenna and the reading usually takes several seconds. Some

solutions [DigiD.dk] use the NFC reading as either a means to elevate LoA of existing PKI Mobile ID or as an authentication of high risk transactions.

- Server-based mobile ID: In this approach, secured identity and authentication information is stored on an external server, which can be accessed using a mobile phone. This solution is implemented in Austrian government m-identity scheme.

When it comes to the adoption rate of mobile ID solutions, it is clear that the growth is much faster than for traditional e-ID card based solutions. The Austrian („Handy-Signatur“) as well as the Estonian mobile eID („Mobiil-ID“) were already extensively used for online authentication for electronic services (e.g., e-government, e-banking). Austrian model does not require any additional hardware and can be used on any mobile phone. The eID data are stored in the mobile ID system's database in cloud, not on the mobile phone. There are more than 500,000 active mobile ID users with 10,000-15,000 uses per day and in a matter of fact mobile ID activation was 15 times higher than traditional eID card activation. Estonian mobile ID (not to confuse with Smart-ID which is also mobile Id solution, but without chip, see above differentiation regarding storage possibilities) relies on the SIM-based approach because at the time it was launched there was a lack of NFC devices in the market to reach a significant percentage of the population. The SIM card uses the same PKI as the eID card and the credential data is stored on a secured SIM card in the mobile handset. Citizens in Estonia access broad range of from their Mobile. 99.6% of banking transactions in Estonia are now done electronically and the country was the first in the world to allow m-Voting in the national Parliamentary elections with 3% of all votes conducted via mobile phone with help of Mobile-ID (Mobiil-ID), already launched in 2007 as an extension of the digital ID scheme. Mobile-ID can be used with over 300 organisations in both the private and public sector, according to e-Estonia.com, with around 40,000 users.

Closer to ARIES pilot with Spanish e-ID card is German contactless eID card and its use with NFC mobile phones. The German Federal Office for Information Security and the Bundesdruckerei has identified several smartphones and versions of Android middleware and applications that enable the German eID card to be used to provide mobile identification and authentication services to German citizens. The Open eCard [16] open source initiative has developed an Android app that uses the German eID card for cloud authentication. Ageto, company developing eGovernment software that supports the German eID card, also released an Android middleware. Other clients include Ausweisapp, PersoApp (PersoApp-eID-Client, Open-Source-eID-Client), eIDClientCore and FutureID-eID-Client (OS-eiD-Client). The structure of the eCard-API-Framework is sub-divided into the following layers:

- Application-Layer
- Identity-Layer
- Service-Access-Layer
- Terminal-Layer

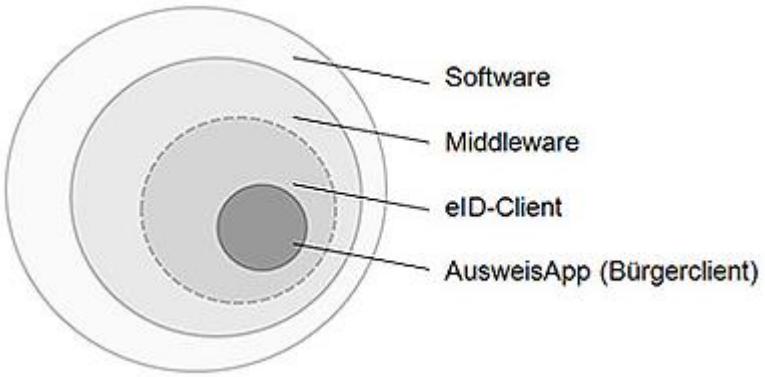


Figure 8: German e-Id client layers

This layered approach, also exemplified in figure 8 (taken from [17] enables extension of supply side of e-ID ecosystem to different providers. In regard to ARIES exploitation strategy, that also relies on stratified and

modular offering, with interchangeable proprietary components and open source APIs, we conclude that close observation of standardization initiatives, including FIDO and GSMA (see also WP6), should be done.

5.1.3 Identity brokers

As mentioned before, in ARIES ecosystem there is also possible role for brokers, such as Identity Attribute Aggregators which act as intermediary between SPs and end user information stored in authentication and attribute providers.

Some EU projects, such as FutureID were trying to expand the scope of typical identity ecosystem by introducing the role of identity broker, in order to support all possible current and future credentials, including non-notified eIDs in a variety of sectors (like BankIDs and corporate IDs), as well as eIDs with a considerable user base. Besides massive scale, support for heterogeneous perceptions of trust, chain of intermediaries (that rely on credential derivation similar to ARIES) and openness were all considered as the project legacy that also are considered in ARIES. However, specific "elements" of ecosystem, namely platform and some of the components are essentially different in ARIES ecosystem. Identity brokers have also been proposed in other EU projects and initiatives, for example Personalized Identity Management Ecosystem Infrastructure supporting Individualized Digital Identities (INDIs). The INDI ecosystem was targeting privacy enhancement by giving individual persons the ability to control with whom they share their identity data and under what conditions, while acting in a private, public or professional capacity themselves or through an authorized proxy. In their business model the role of intermediate operators in a market for privacy-aware identity services was offering individual choice that differentiate from current data aggregation practices of commercial actors. The role of brokers will be further explored in ARIES.

In most existing projects or initiatives the government issued e-ID card is the first means of the authentication (primary or mother eID) for subsequent enrolment of other credentials with lower level of assurance. The new credential is created can be afterwards used independently. In most cases the link between the credential and the user is stored only in IdP database with audit log information about the creation. In ARIES this is the role of Secure Vault. This is the first type of "derived credentials" where the mobile PKI token is only credential and the attributes are acquired from backend attribute source, provided by the IdP. This solution, however, has several weaknesses, for example identity provider stores all the information and manages all policies and private data sharing policy always relies on the IdP.

The concept of derived credentials and virtual IDs fits well with identity broker model. Derivation can be split into two categories, remote provisioning and local provisioning. In remote provisioning user performs an ID card authentication towards a derived credential issuer or broker system. Once the authentication is successfully performed, the user downloads the derived credential from the issuer. In a local provisioning user taps the ID card on the mobile device which is accessing the ID card or ePassport via NFC and triggers a derivation of credentials from the ID card. Enrolment of new virtual IDs through broker might have different levels of assurance (link to real user identity), as well as policies to verify additional information such as biometry during authentication in case of suspicious behaviour. Additional attributes could be requested and submitted by the user as well as external providers, thus providing different levels of non-ID attribute assurance. Some of these issues can be treated directly by a virtual identity provider, but in some cases identity broker might be preferred. Architectural separation of two functions of IdP removes the threat of tracking of user activity among SP, as it was describes in D3.1.

Examples of brokers-like networks include Finnish Trust Network (FTN), which is a cloud-based mechanism for connecting large scale, consumer facing services with trusted identity and service providers. The Finnish Trust Network not only relies on eIDs issued by the government but also recognizes the electronic identities issued by commercial identity providers such as banks and mobile operators. In Germany SkIDentity Service (skidentity.com) is a kind of broker for service providers that can use popular social logins such as LinkedIn and Facebook Login, as well as eIDAS eID services from a number of countries. eIDAS brokerage was activated in 2017 and now enables strong authentication and identification with support for various international identification documents in cross-border processes. In Netherlands, similar broker role to municipal e-services

is provided by Connectis with support from CEF project (https://eidas2018.eu). The 81 participating municipalities opened up 200 public services to European citizens and representatives of Dutch businesses in the possession of an eID. The other brokers envisaged in the project, which is under the lead of Dutch Ministry of economic affairs, include Digidenity and KPN.

5.1.4 Community based trust

Trust framework is a term that has different meaning for different people. The most widely used definition is from OIX [18] that refers to "legally enforceable set of specifications, rules and agreements regulating an identity system." It goes on to define the relationship between a trust framework and the underlying, regulated identity system, as well as the context in which the trust framework exists, so in a sense we could say that eIDAS is also providing trust framework. In more recent NIST paper [19] it is mentioned that "the rules for federated identity management are known as trust frameworks and the organizations that agree to follow such rules and participate are known as identity federations". They also cite Whitehouse paper on national strategy for trusted identities [20] that states "A trust framework is developed by a **community** whose members have similar goals and perspectives. It defines the rights and responsibilities of that community's participants in the Identity Ecosystem; specifies the policies and standards specific to the community; and defines the community-specific processes and procedures that provide assurance. A trust framework considers the level of risk associated with the transaction types of its participants; for example, for regulated industries, it could incorporate the requirements particular to that industry. Different trust frameworks can exist within the Identity Ecosystem, and sets of participants can tailor trust frameworks to meet their particular needs. In order to be a part of the Identity Ecosystem, all trust frameworks must still meet the baseline standards established by the Identity Ecosystem Framework".

In line with the projection of trust frameworks and even whole identity ecosystem to a single community (e.g. sector specific), we observe that relying party (service provider) might impose some requirements for the credential to be presented, including provided attributes about user identity and trust requirements. On the other hand user can choose the mechanism and credential he wants to present according to his preferences and those requirements from SP. This could include the following options:

- usage of a derived credential with less identity information and/or a pseudonym;
- a proof of identity in which no credential is actually sent to the SP, but a proof that the user owns some identity or attribute; or
- a Mobile ID credential stored in a secure element, which makes use of the Trusted Execution Environment for authentication and can optionally involve mobile operator as party involved in circle of trust

Sector specific e-ID schemes, ecosystems or frameworks have been relying on identity management system with limited scalability and only recently some sectors (banking, postal etc) started with adoption of light-weight e-ID protocols. In addition decentralized approaches, like some of those mentioned in chapter 5.1.1 are starting to be adopted by web specific communities. Uport [41] is an example of Open Identity System for the Decentralized Web. It is mainly known as a system that allows users to register their own identity on Ethereum (similar virtual money scheme to Bitcoin), send and request credentials, sign transactions, and securely manage keys & data. Similar platform is Jolocom [42] , which is part of the Deutsche Telekom T-labs project aimed at building full block chain based stack of services. CULedger, builder of innovative blockchain-based products for credit unions and their members, teamed up in 2018 with Evernym [43] to launch MyCUID, focused on credit union members, enriching the trusted relationships members have with their credit unions.

The importance for ARIES in relation to sector or community specific solutions is mainly related to the exploitation of sector specific customized platform such as eCommerce and Smart Airport, and the need to investigate further requirments for the establishing of specific trust framework.

5.1.5 Identity fraud and citizen attitudes

Recent study shows that of the 3.1 million complaints received in 2016 by Consumer Sentinel Network [5] , which is operated by the US Federal Trade Commission (FTC), 1.3 million were identity fraud related, costing consumers over $744 million. The median amount consumers paid in these cases was $450. Strengthening the link between physical and virtual identity for both individuals and legal entities, and considering different levels of assurance, including privacy-preserving and anonymization capabilities, is therefore an important step that will enable stronger involvement of LEA in the identity fraud prevention.

According to another study issued by Forrester [6] , 66% of respondents state that customers are demanding stronger online security and privacy protections. This study also lists several trends will have a dramatic impact on eID budget priorities, architectural decisions, the vendor landscape, and deployment options. They also claim that this sub-segment, also named consumer identity and access management (CIAM) will grow by 22% between 2017 and 2018 and will reach 713 M dollars.

Regarding the threat landscape and attacker tactics, both IBM and Verizon have published reports describing how attacks have evolved. Verizon has distinguished 9 patterns over the last 10 years. IBM defined 10, including one called undisclosed. Looking at those patterns, 7 out of 9 are identity and access related. From session hijacking, privileged access control to misuse of certificates, i.e. cryptographic material.

Solutions like role based access control, a central identity repository and enterprise SSO are either outdated, cannot provide the correct security mitigations or cannot be justified from a business case perspective. The point is that those 'legacy' technologies do not give the answers on the questions being provided by the mega trends mobile, social, big data and cloud.

GSMA published an October 2015 survey [13] of 1,000 consumers that provided statistics on how consumers answered the following question: "What documents or processes do you expect to store, or carry out, using your mobile phone by 2020?". The responses are shown in Table 3.

Response	Consumers (%)	Response	Consumers (%)
Making a payment to an online store without cards	50	Storing loyalty cards and coupons	48
Tickets for travelling on public transport	35	Registering or sharing information with your doctor	35
Actively protecting yourself, your home and your family from hacking and fraud	33	Authorizing access to home Internet and TV	33
Storing your driving license	28	Proving your age when purchasing alcohol or cigarettes at a self-service check out	24
Filing your tax returns	23	Voting in elections	22
Entering your place of work, VPN, printers	19	Entering a country using a passport	17

Table 3: user preferences for mobile phone storage of documents

In regard to identity fraud, many governments started or speed-up eID initiatives. In Nigeria, where there are estimates from the country's banks that they lost 159 billion naira ($800m) to electronic fraud between 2000

and 2013, eID card with Match-On-Card technology has been launched. It matches a holder's fingerprint against a profile stored in the embedded chip and it can be used as a form of payment, since it was realized in cooperation with Mastercard. This combination of the identity scheme with a strongly commercial initiative such as the bank card is the main cause for privacy concerns, however.

In Ponemon institute study [22] two figures are especially interesting for ARIES analysis. The first one is on effectiveness of approaches to stop unauthorized access to information resources. While 74% agrees that a single factor authentication is no longer sufficient to effectively protect access to online services, only 50% believes that multi-factor authentication is the right answer and is effective at reducing risk posed by identity fraud. So what the other 24% respondents thinks? Should at least one of the factors have higher level of assurance?

5.1.6 Support for Law Enforcement

In this increasingly globalized world where everyone is interconnected, we haven't still set the technological measures to fully assure and support law enforcement related to e-ID. As a result of this, identity related crimes (theft, impersonation, etc.) are on the rise. Moreover, recent terrorist attacks have revealed that border police officers can be easily tricked by criminals in their way to enter or to escape to/from a country, just because the only verification carried out is a visual check of a passport or a national identity card. Obviously this is not enough and this is where technology can help in cases like the identification of criminals, or preventing the commission of future crimes including online fraud. A solution based on a link between valid identity cards and biometrics (like in ARIES) would be the gold mine to sort the matter out.

LEAs are aware of the use of e-ID technologies and new opportunities related to mobile phones, such as use of cameras or biometric sensors. Facial recognition, voice and fingerprint are widely used in these devices, and customers are already familiar with them, so the support for increasing LEA capacity related to this new form of e-identification is very important.

Some LEA experts in ARIES project consider the existence of two different sets in biometrics, one of them would be physiological (physical characteristics; namely face recognition, fingerprint, iris, etc.) and the other would be what is known as behaviometrics (gait, typing, voice, etc.); the trend is to combine more than one biometric feature (multimodal biometry) to achieve a successful identification. In addition, new solutions based in blockchain are arising in different fields related to biometrics, in order to strengthen privacy and security, such as health, commercial agreements, identity cards, border control, logistics, regulated supply chains, banking, energy, industry and so on.

Other LEA experts stress importance of two factor authentication, along with a portal which has direct links to other Government agencies databases. An example is scan a passport, directly checked against the relevant database with auto facial recognition, detail comparison etc, similar to the new smart passports deployed at some airports. This technique, coupled with a number of other suitable ID documents would be sufficient to confirm ID.

The other key trend and need related to LEA investigation support is interdependencies of accounts, often designed to make a consumer life easier, but it could present difficulty when it comes to forensic investigations. Other challenges mentioned by LEA are:

- Wide scope of products with lack of generic support or common standards
- The applications, services or apps all differ in selection of security mechanisms or implementation of these mechanisms
- Lack of clarity when it comes to issue of LEA role and responsibility regarding advises to the general public (e.g. not to use a commercial service)

In order to support the LEA's in prevention and detection of online crime, industry standards could be introduced like a Kite mark [52] . In addition, support for identity theft or cybercrime awareness could follow approach similar to the UK crime prevention 10 Principles advice. These principles, ranging from target hardening, to deflecting offender, could be also adapted for digital world.

5.2 *Supply side analysis*

ARIES technologies are diverse and on supply side there are important competitors, alternatives and trends to have in mind for the project results packaging and positioning. Existing and established biometric verification from mobile devices and anti-spoofing solutions (e.g. live face detection) are, for example, increasingly present on the market, while demand for specific identity proofing and verification (IPV) solutions, separated from the overall identity management, is driving innovative technology supply that can become either competitor or substitute for this part of ARIES system.

5.2.1 Identity Proofing and Verification

In ARIES identity proofing and verification (IPV) refers to a process that combines providing identity evidence with a number of checks: checking it in order to determine whether it is genuine and/or valid (validation), comparison of provided evidence and/or knowledge about the Claimed Identity to determine whether it relates to them (verification), checks to determine whether it has had an existence in the real world over a period of time (activity history), checks with various counter-fraud services. Finally the sub-system that performs identity proofing service delivers an assured identity that describes the level of confidence that the applicant is the owner of the claimed identity and that identity is genuine. Therefore, we use term "assured identity level" or simply "identity assurance" for the final result of identity proofing process.

In essence it is all about performing number of checks, by combining visible end electronic domain security features. Terminology, however, can be confusing: in ARIES identity verification is only one step of the overall proofing process, in line with definition provided by UK Government guide [7] . Note that identity proofing and verification is only part of the enrolment and issuing process. This guide, for example, is also stating that "assured identity levels" it defines (from level 1 to 4) only cover identity proofing and verification processes, and therefore cannot match exactly standards for "levels of assurance" (LoA), such as NIST [9] or more importantly European eIDAS guidance with low, substantial and high LoA [10] . With this "disclaimer" and a table that is presenting relationship, and not correlation or direct mapping, to the existing identity proofing and verification standards, UK Government guide [7] is developing further notion of "assured identity levels" with Level 4 described as "Level 3 Identity that is required to provide further evidence and is subjected to additional and specific processes, including the use of Biometrics…"

It should be also noted that "identity proofing" and "identity verification" are sometimes used in a different order or at the different abstraction levels. In [8] for example, identify verification system is defined as "that provides access to facilities or data typically performs activities such as:

• Identity proofing

• Identity authentication

• Authorization"

However, the predominant definition of identity proofing and verification (IPV), as a separated e-ID, market sub-segment, is focusing only the initial validation of an identity of an individual (that an applicant for an identity credential is in fact the person the applicant claims to be). In ARIES we consider authentication and authorization activities separated from identity proofing and verification, in order to align with this trend.

Robust identity proofing requires the user to present identity documents and information in-person as part of an online service or on-boarding process. A biometric enrolment and search performed serve to ensure, for example, that the applicant is not already registered in the system, perhaps with different identity information.

Considerations for comparison of identity proofing methods or solutions at the market include:

- Strength of identity evidence e.g. e-ID card versus Id card without chip
- Validity of identity evidence and data
- Verification that user is owner of the identity evidence e.g. only by having access to evidence or by biometric verification

- Controls on counter-fraud, activity history, accuracy…

Static verification or shared secret, for example, requires that the user and the proofing organisation have a pre-existing shared secret, or that the proofing organisation uses an external trusted source with which the user already has a shared secret. Dynamic verification or challenge/response method needs the proofing organisation to gather information and then requires the user to demonstrate that they have knowledge of it. The physical comparison method of verification is relevant for ARIES, since it requires the user to be verified by a visual confirmation that they appear to be the person to whom the Identity Evidence was issued, therefore producing high cost for face to face checks. Finally, biometric comparison is type of verification that requires biometric confirmation that they appear to be the person to whom the identity evidence was issued. Remote biometric verification like in ARIES, is the currently the most promising method.

The term Identity Proofing and Verification often refers to different technologies in USA and Europe, for example. Some can be fairly simple using just a REST API to verify that a particular combination of personal information attributes (like name, address, email, phone, etc.) have been seen or checked out somewhere before. In Europe e-ID card and biometrics are increasingly used, while in USA many services rely on databases. Legislation requirements are also different. While in Europe we have GDPR, HIPAA compliance is very important in USA. One of the biggest ID verifications software in USA is Jumio [26] while the other include Shufti Pro, Trulioo and Onfido. Jumio technology called Netverify is also delivered as a service, and company coined the term Trusted Identity as a Service (TIaaS), that is combining the three core verification pillars: ID card Verification (by extracting data from image of an ID card), Identity Verification (selfie and biometrics) and Document Verification (similar to ID verification but using manual verification by document experts). IPV service provider market is also including techniques not related to ARIES, for example verification by questions only specific users should be able to answer. Payment Instrument is technique where company makes a small deposit in user's account and then user must confirm this amount. Even social media profiles are used by some service providers for identity proofing and verification (although it is obvious that the profile can be fake). Companies like Experian, Equifax or Lexis Nexis are important IPV service provider, mainly providing services to financial institutions. Mitek [44] is another company with specific focus on financial sector, however, with technologies similar to ARIES, including NFC verification of ePassports. Kofax solution [45] , on the other hand, relies on optical character recognition (OCR) and patented image quality enhancement technology. In a matter of fact, many technologies used by IPV technology providers, such as machine learning or signal processing, are patented.

An example of technology based solution for mobile identity proofing involves camera that can capture an image of government issued document (not necessarily eID or ePassport), which then can be used to support identity proofing. In order to confirm that a customer who utilises a biometric to login is in fact a real person and not an imposter, liveness detection is utilised. Liveness detection uses a number of technologies to confirm that the biometric belongs to a living individual depending on the biometric used. This type of identity evidence verification is the most basic one and is also referred as DV1 level (document verification level 1) in Gemalto brochure [11] from which figure 10 is extracted.

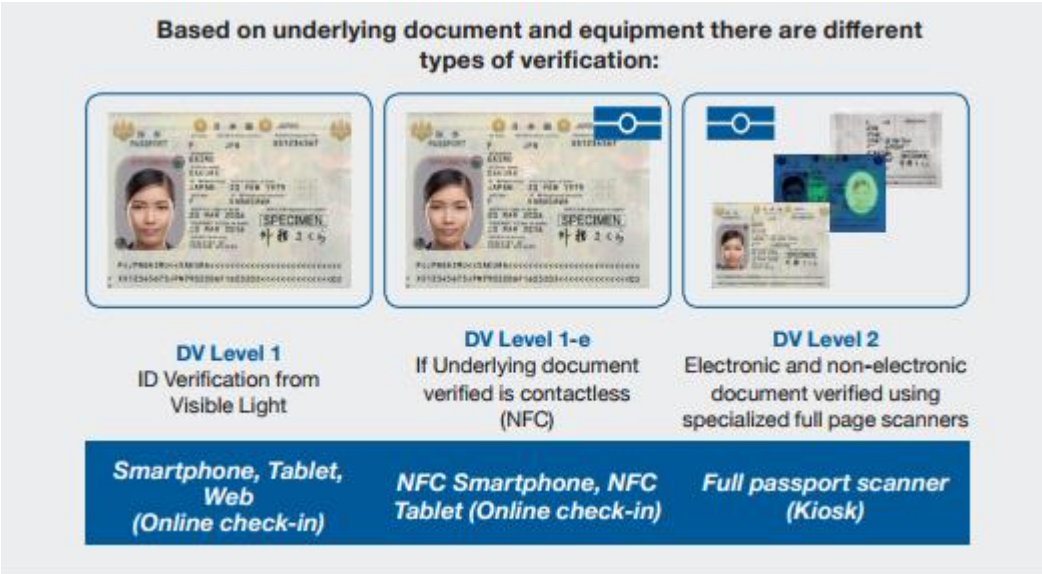


Figure 9: levels of document verification according to Gemalto brochure [11]

AriadNEXT's facial recognition service [23] , is one example of DV1, and it ensures that the person who subscribes to a service is the one it claims to be by comparing selfie taken by mobile phone with picture from eID card. In a matter of fact, local biometrics via mobile phone is now widely accepted since it provides good usability and higher identity assurance. Another French start up, Chekk [25] , uses both on and off line e-Id verification, as well as face matching with liveliness detection, and more traditional PIN, password and fingerprint verification methods. However, it also uses mobile data wallet app, similar to ARIES, to control data users share, and to create personal profiles combining identity data and attributes. Its selling proposition is also mentioning saving form filling time for users, as well as encryption at a user and data level.

ARIES identity verification is positioned at DV1-e level, where electronic data is transferred through NFC protocol and used for document verification, next to biometrics. In case of verification with Spanish eDNI, the most similar application is Authada [24] that works with German e-ID card. It is still not clear how it is positioned versus new platform Verimi [28] that was mentioned in supply side analysis and that is backed by many large organisations and service providers. VERIMI is more similar to complete ARIES system since it manages all identity lifecycle and pretends to build an ecosystem. As opposed to AUTHADA IPV technology, in ARIES a duplicate check is performed, a biometric enrolment digitally links the users trusted unique record to them physically through their biometrics. This biometrics can then be used perpetually to prevent future attempts at false representation of their identity information by a fraudster. While biometric identity proofing requires additional effort to verify identity data integrity and detect duplicate enrollments, it provides yet another very effective barrier to fraud. NFC interface of Spanish DNIe 3.0 has been explicitly designed to provide compatibility with the ICAO ePassport and therefore allows to read public identity attributes without the need to use the PIN mechanism (needed to authentication and digital signature), with any NFC-enabled smart device. The electronic data structure of the DNIe is equivalent as well to that of the ePassport, and therefore the DNIe can be used as a Travel Document also in eGate/ABC systems at the borders in an equivalent way to the ePassport (which is also relevant in the domain of Airport piloting in ARIES).

Finally, there is a third type (level DV2 in figure above), which includes verification used in airport kiosks (so called automatic border control or e-Gates) that incorporate scanner technology. There are many implementations of this technology, with leading vendors in the market being Gemalto, NEC, Idemia, Vision-Box, AOptix, Atos, Automatic Systems, Ayonix, eGate Solutions, and SITA. In relation to this type of IPV, Technavio has published its latest market research report on the global automated security e-gate market,

which examines key trends expected to impact the market outlook from 2017-2021[3] and envisages compound annual growth rate CAGR of 9% in this period. This type of verification is not applicable to ARIES use cases, so we will not analyse it further.

Biometric authentication is referred either as "in-band" or "out-of-band" verification method, depending whether it is performed via a parallel channel that is independent of mobile device transaction. Out-of-band authentication is performed as a separate, parallel function to the transaction. There are different approaches. An authentication might rely on the user providing information provided via a separate, parallel channel, such as by sending an access code in a text message or email that is then used to gain access, with biometric authentication performed out-of-band by an accompanying human being processing the transaction. Out-of-band mechanisms add yet another layer of security, requiring access to a device, e-mail account, or in the case of accompanied processing, physical presence (which also affords an opportunity for facial recognition by a human, document checks, etc.).

When it comes to mobile phones, verification is device specific and constrained to operate as implemented by device, OS, and application suppliers. While organizations aim to standardize architecture and interfaces, biometric functionality and performance will not be universal or configurable on these devices, and will not necessarily meet the security requirements of a particular application. In the next chapter we examine trends and standards in mobile multifactor authentication.

5.2.2 Multi-Factor Authentication

Multi-factor authentication is essential to elevate level of identity assurance and therefore improve security. It requires at least two of the usual three factors: what the user knows (e.g. PIN), what the user has (e.g. secure token), and what the user is (biometric). The authentication factor (e.g. PIN) should be stored securely and accessible only to the user; local PIN verification between the local secure token and the reading device is preferable to verifying the PIN remotely over a network. Ideally the user should be able to tell if possession of the authentication factor is compromised. Note that some organizations do not consider local PIN as an additional factor and explicitly request to have additional authentication with the server.

The most common multifactor authentication mechanism still in use today consists of a small hardware device or token assigned to a user, and which generates an authentication code at fixed intervals. The new generation of tokens can be plugged into a USB port to provide the authentication code directly to the host system. Another common method, frequently used by financial services is to use a text message code or one-time passcode (OTP) for out-of-band authentication, providing an additional layer of security. Modalities such as SMS and voice OTPs, however, are used less and less and are increasingly replaced with solutions that rely on hardware incorporated into new mobile phone generation, whether it is chips inside, cameras for capturing QR code or interfaces for capturing biometric traits.

Using the mobile devices as authentication factor also includes a possibility to use generic QR-based authentication framework. The framework is based on the user's identity stored on his smartphone (as the user's authentication factor) and a dedicated QR Authenticator component (as the user's identity verifier). An identity transfer has been realized from the user's smartphone to his desktop by using QR codes. The identity of the user is intended to be known only to the QR Authenticator but not to Service Provider. In this case, the model may provide also the user privacy-preserving if the QR Authenticator is a trusted party for the user and it not reveals the user's identity to the Service Provider.

[3] https://www.technavio.com/report/global-automated-security-e-gate-market

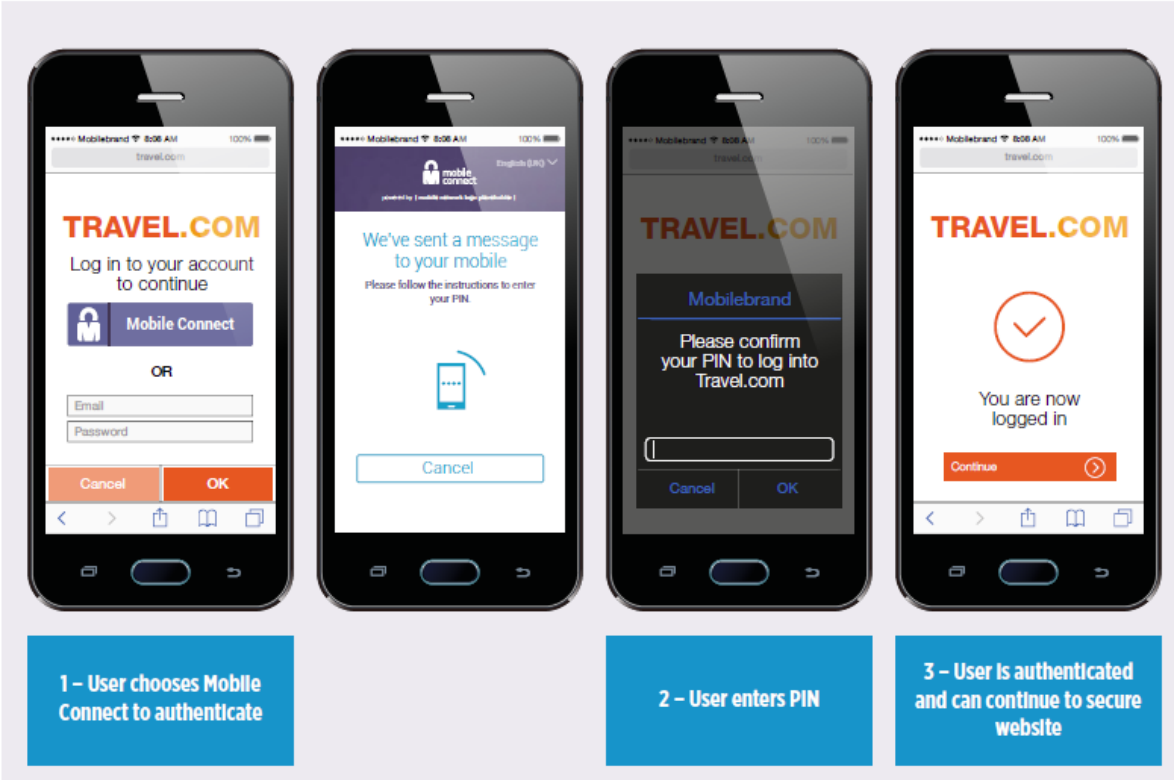


Figure 10: Mobile Connect authentication steps

Mobile Connect [27] is e-ID scheme supported by GSMA that can combine mobile device associated with a unique mobile number via the SIM card and PIN code to verify and authenticate the user. This is the way that Mobile Connect supports two-factor authentication, relying on out-of-band authentication (the use of separate devices or channels for "consuming" the service and authentication for service access). Mobile Connect uses the standard Level of Assurance (LoA) definitions from ISO 29115 for authentication: a global standards-based approach to authentication security. LoA3 is a high-security two-factor authentication solution. LoA4 requires, in addition to LoA3, that the security credentials are based on PKI technology. In practice, LoA3 is comparable to European eIDAS directive defined security level "substantial" and LoA4 is comparable to "high". Within the Mobile Connect framework, LoA3 service is typically achieved using a SIM applet with security credentials placed on the user's mobile phone SIM secure element, together with strong encryption for messages to and from the SIM. For LoA4, the SIM applet has PKI security credentials. There is a theoretical difference in security between normal (symmetric) and PKI credentials (asymmetric), but in practical day-to-day use, the difference is negligible. In fact, the use of additional security features, such as mobile operator business processes and dynamic mobile network data, may be more effective in increasing overall security and fraud resistance than by the addition of PKI certificates.

Until recently, biometrics were not considered as a suitable factor for mobile eID verification/authentication as consumer grade biometric readers on mobile phones were without replay protection and no liveness detection. However, this is changing with the new generation of mobile phones. In addition so called fourth factor (where you are, revealed through geofencing or location awareness) is increasingly used in so called risk-based authentication.

In the previous chapter on demand side analysis we saw that mobile eID is gaining traction. Advantages of the mobile multifactor authentication based on mobile ID are clear for both demand side stakeholders: citizens chose it for convenience, while service provider can rely on better security mechanisms thanks to the recently adopted technologies. An example is already mentioned Smart-ID, an Estonian solution that can be used on both smartphones and tablets without mobile internet connection, or special SIM cards. Touch ID is currently

not supported by Smart-ID, but according to the solution owners they are considering adding biometric support for Smart-ID in future

The ID on the mobile device can also be used to perform multi-factor authentication in different categories:

- Authentication to another mobile device or terminal, for example building access or boarding area at the airport
- Authentication to a remote server or cloud service, such as eCommerce, for example FIDO or GSMA Mobile Connect.
- Authentication to another local application, on the same device, for example a Bring Your Own Device (BYOD) container service.

All of these use cases are also considered in the section 6, although BYOD scenario is not considered in ARIES pilots.

5.2.3 Secure storage and processing in mobile phones

In regard to mobile phone storage three models leverage on near field communication (NFC) protocol to support so called contactless mobile wallets:

- secure element (SE) embedded in the mobile phone
- host card emulation (HCE) software that replaces the SE in the mobile phone while secure tokens are downloaded from a cloud server and stored in the mobile operating system (OS).
- trusted execution environment (TEE), which is a secure area of the main processor in the mobile phone that can also be used to store secure token.

Variations to the first option are most applicable to existing m-ID initiatives. Secure Element (SE) can be considered as an environment to store data securely, process data securely and perform communication with external entities securely. Similar to smart card or SIM card, it is a tamper-resistant platform, that comes in three different forms: Universal Integrated Circuit Card (UICC), embedded SE and microSD. Each form factor links to a different business implementation and satisfies a different market need.

SE technology is coming from well-known and used (at least in Europe) EMV smart card technology, tested against a set of requirements defined by the main payment networks. Fraud opportunity is limited to a single with only a small amount of data is stored on them (single customer credentials and device specific cryptographic information). HCE technology on the other hand assumes that any data stored on a handset is vulnerable and therefore restricts the storage of sensitive data to host or “cloud” databases. Difference is obvious when it comes to management and control of identity data. With SE based solution a client must control secure storage, manage locally available data, trigger updates etc. SE is less reliant on mobile networks availability, but not all mobile phones have SE. Apple Pay, for example, uses a hybrid solution, while many other service providers, such as mobile payment providers, use HCE with tokenization, device fingerprinting, risk modelling and additional on-device verification software.

The least popular option seems to be use of trusted execution environment (TEE for credential storage, although the TEE is used more frequently for data entry and display, and for processing of services in order to establish higher levels of security assurance. Here, decisions should focus on processing power and storage, as opposed to the level of identity assurance requested by service provider.

e-SIM is another technology trend to watch in the near future. It presents mobile users with many available operator profiles and over-the-air provisioning once a network is selected. Machine-to-machine (M2M) applications have used similar solution for built-in SIM cards for several years now and it is expected that e-SIM market will grow rapidly and that the value chain as well as identity ecosystem will change. SIM manufacturers will negotiate with mobile hardware providers directly, and preconfiguration and profile-

handling services will become more important in the value chain. Existing internet identity providers such as Facebook or Google are already used by many e-service providers instead of mobile phone number (SIM card), for example voice services via a data connection. Google's Project Fi, for example, is mobile virtual operator (MVNO) offer, recently launched, that strives to provide the best available data-network performance on mobile devices by combining mobile data and Wi-Fi connectivity. It automatically switches between networks depending on signal strength and speed and connects to open Wi-Fi hotspots while securing data with encryption through an automatic virtual private network. Phone calls, if placed over a Wi-Fi connection, will seamlessly transition to a cellular network if Wi-Fi coverage is lost.

5.2.4 Mobile biometrics

Because entering text on a mobile device can be error-prone and cumbersome, it is often more effective to authenticate a user on mobile device without text passwords, such as by requiring the user to connect sequence of points or by biometrics. Market adoption of mobile biometrics is principally following boom of mobile payment solutions. Apple Pay is the leader with Touch ID and the contactless reader. It relies on a fingerprint recognition sensor that is available for all newer device models starting from the iPhone 5S and newer iPad models. Google Face Unlock was introduced in 2011 as part of Android 4.0 (a.k.a. Ice Cream Sandwich). The service uses a front-facing camera to capture an image of authorized users. This feature became Trusted Face with Android 6.0 (Lollipop) and provided significant usability improvements. Google Trusted Voice was available in early 2015, while Samsung Galaxy Note 716 contains a feature that allows users to unlock the device with iris scanning.

Acuity claims [29] that by 2020, 100% of all mobile devices will have embedded biometrics. Because there are many different ways of proving biometrics, a standard way of integrating authentication into a system is needed and this is where Fast Identity Online (FIDO) is doing standardisation by specifying the Universal Authentication Factor (UAF), an online client/server system that abstracts an authenticator relying on a challenge/response protocol. Besides FIDO, there are other options, namely W3C Web Crypto API, EMV 3D-Secure protocol that is focused on bank card issuers to authenticate consumers directly for online, or even client-based TLS Certificates, defined in the Internet Engineering Task Force (IETF) RFC 5246.11 that, however, is more used in VPN or authentication of websites with smart cards or desktop certificates.

Like all security mechanisms, biometrics are theoretically vulnerable, but the barriers are high and are getting higher with new liveness detection technologies and other techniques that make spoofing unattractive to the vast majority of even the most talented and ambitious fraudsters. One provider that uses liveliness detection technology is Facebanx with live streaming technology that combines face and voice recognition and document verification.

5.2.5 Privacy-preserving identity management technologies

Traditional IdM systems do not provide means to their users to deal with the data minimization principle, which is a core aspect of the recent General Data Protection Regulation (GDPR). Moreover, the usage of certificates does not preserve anonymity since entities are unequivocally identified in the certificate that is entirely disclosed to the other party. In contrast to these approaches, Anonymous Credential Systems (ACS) [30] , such as Idemix [31] or U-Prove [32] , allow users to present cryptographic proofs, instead of the whole credential, proving the possession of certain attributes or claims.

These systems enable a selective disclosure of identity attributes to achieve a privacy-preserving identity management approach. Indeed, a user or entity can prove a specific set of properties associated with a subset of identity attributes, without disclosing the content of such attributes itself. Nonetheless, despite some important initiatives and projects, such as PrimeLife [34] IRMA [35] or ABC4Trust [33] have analysed the use

of ACS-based and privacy-preserving identity management systems, these technologies are not broadly used in the society yet.

Anonymous credentials systems are being currently be adapted and improved to be deployed in mobile scenarios, as it is being doing in ARIES and some other projects such as Irma [35]. IRMA, like in Aries, offers a way for privacy-friendly authentication based on Idemix. When authenticating the user reveals only relevant properties (attributes) of himself, using an IRMA app on his mobile phone.

In this context, another trend is to deploy and leverage Anonymous Credentials Systems to cope with the Internet of Things (IoT) [37] . Unlike in traditional scenarios, in IoT, a huge amount of smart objects are enabled to interact with each other, so an explicit user consent for each interaction is not feasible, due to scalability reasons. Furthermore, such smart objects could lack user interface, and consequently, human interaction should be maintained at the minimum.

Anonymous credential systems are also being introduced in decentralized ledgers and blockchain solutions. In this sense, emerging blockchain solutions such Sovrin [39] and uPort, propose a decentralized ledger that empower users with mechanisms to preserve their privacy in their digital transactions. Identity Management (IdM) systems for blockchain are switching from traditional web-centric approach, towards the self-sovereign identity paradigm to empower citizens to take control of their data in any-time in any online situation. Thus, user personal data is no longer maintained in third-parties services and information regarding transactions and interactions of users in services can be anonymized by integrating anonymous credentials system like [31] in the blockchain platform. It avoids that third-parties can leak personal data, and, in the worst case, become a potential source of other, more important, risks, such as identity-related cybercrimes (e.g. identity-theft).

In the upcoming IdM model, identity attributes will be kept protected within a trusted module inside user's smartphone, whereas the corresponding user's public keys are managed in the IdM system placed within the permissioned blockchain, such as for instance, ALASTRIA [40] . It will provide a distributed system that enables identity verification of user's claims about their attributes and any associated asset, enabling provenance of the claims.

Privacy-enhancing technologies are starting to bring many benefits as they are introducing in different markets. Disparate kind of scenarios will benefit from this technology. When placed in the blockchain, privacy-preserving solutions will shake up and boost many sectors and markets, such as: Citizen Digital Services, Healthcare, Consulting Services, Energy, Engineering & Construction, Financial Products & Services, Insurance, Legal Services, Legal Software, Media & Digital Marketing Products, Telcos, Travel Product & Services.

Furthermore, in the future, evolved versions of Aries solutions and technologies might be integrated in eIDAS nodes, in order to achieve an interoperable and trusted connection across IdM services, Service Providers and users across Europe. The user’s attributes managed in the IdM and the mobile, would be obtained from attribute providers within the eIDAS ecosystem. Likewise, claims and attestations about those attributes as well as authentication might be accomplished according to trusted eIDAS ecosystem, e.g. through the Stork infrastructure.

6 Use of vID

The concept of virtual identities has been evolving over the years, together with the evolution of internet, web platforms and virtual spaces. Early definitions were referring to "avatars", a kind of representative image in a video game, while name e-identification ("eID") was reserved for an electronic identification solution of citizens or organizations, sometimes in the form of smart card provided by government authorities, banks or other companies. Terms digital identity and online identity are also often used to refer to set of attributes about a person or even collection of information generated by a person’s online activity. This includes usernames and passwords, but in some cases englobes online search activities, purchasing history etc. In this chapter we will analyse the widest possible definition, covering all possible types and uses of data that is representing a user in online world. Generally, the proof of identity that is required to gain access to something is proportionate to the value or risk related to service being accessed. While services related to vID, namely

identification, authentication and authorization, in this chapter we will mainly analyse the impact of authentication alternatives in different sectors. We can distinguish:

- One-time password - process where a user's password and information is used for logon and then, becomes invalid after a time.
- Two-factor authentication and Multi-factor authentication requires that the user uses a user id, password, but also other form of authentication method as smartcard or biometric.
- Physical evidence of identity such as smart card or ePassports, which can be categorised as either memory cards or microprocessor cards.
- Biometric based systems verify the identity of the person by processing biometric data (1:1 comparison). Although the identification function should be regarded as distinct from authentication from an application perspective, often systems using biometrics integrate both identification and authentication functions, since comparison 1:1 in authentication is actually a repetitive execution of the identification.

6.1 *eCommerce*

Among different online service providers eCommerce is especially vulnerable. Fraud and identity theft has been said to be responsible for an estimated 54% of attacks that target e-commerce platforms[4], so the higher levels of assurance while retaining user-friendliness is an important challenge for this type of service providers, especially since shopping is not anymore the only service provided by eCommerce sites.

However, e-commerce risks are not solely about monetary loss. In [46] study published in 2007, 57% respondents say the direct monetary loss from fraudulent transactions is one of the major e-commerce security threats facing their company today, but even more (59%) say they fear the unauthorised use of proprietary or competitive information, and a substantial number (39%) are concerned about the reputational risk.

eCommerce exemplifies area of online services where citizen interests and industry business models collide and mesh. There is ambivalence and confusion over what level of privacy user can expect in which online context. This could be more consequence of the user unfamiliarity or lack of knowledge, for example in eCommerce. While for the most of physical commerce situations, especially when paying in cash, anonymity has been expected by default, in the same commerce scenarios online users can be requested to introduce some personal data.

For eCommerce service providers maximising commercial gain is the main focus, so e-identity is often considered as the source of data that can further increase this monetary gain (e.g. targeted advertising based on attributes shared by online social network identity providers). The link between eID, customer relationship and analytics is frequent in eCommerce context (figure 11).

[4] According to Frost & Sullivan

Figure 11: Use of identity data in eCommerce

Compliance with sector specific requirements (e.g. PCI standard), regulations and legal rules is accepted as a necessary precondition of developing and sustaining trust in the supplier and goods or services being sold. The monetarisation and commercialisation opportunities arising from collecting data do pose, however, serious privacy and ethical questions, as it was stated in deliverable D2.2.

While online transactions through marketplaces, such as Amazon or Alibaba, continue to grow, direct cross-border ecommerce encounters barriers. The EU report on Digital Single Market [4] notes that:

- only 15% of people shop online from another EU country
- Internet companies & start-ups cannot make full use of online opportunities
- only 7% of small businesses sell goods or services across the EU's borders
- businesses & governments are not benefiting from digital tools as much as they might.

The EU's commitment to creating a digital single market relies on eIDs as the building block of what has been already named Digital service Infrastructure (DSI) and is supported by Connecting Europe Facility (CEF) telecom programme. In addition, Commission will make full use of alternative mechanisms under the General Data Protection Regulation (entry into force 25 May 2018) and Police Directive to facilitate the exchange of personal data with third countries with whom adequacy decisions cannot be reached. The other relevant pieces of regulations, such as the second payment service directive (with the introduction of requirements for SCA – strong customer authentication), will create further impact on the market.

In a matter of fact, update of First Payment Services Directive (PSD1) is partially driven by continual rise of eCommerce, as well as technological innovation in payments sector. Second Payment Services Directive (PSD2) is implemented from 13th January, 2018, but the earliest date that member states are expected to have implemented Regulatory Technical Standards (RTS) is August 2019. One of the main challenges is around strong customer authentication (SCA) and guidance around exemptions and challenges. An important element of SCA is two-factor authentication. eCommerce merchants might also need to integrate dynamic authentication tools (e.g., 3D Secure 2.0). It is also expected that eIDAS regulation could complement the additional functionality which is brought in by the PSD2. Account Information Service Providers (AISP) and Payment Initiation Service Providers (PISP) need to interface with existing core banking systems in order to access relevant customer data and provide their services and this is where eIDAS scheme could provide cross-border infrastructure and support for "notified eIDs" recognition, which provide the "high" level of assurance, can be used across the EU to open a bank digitally in any member country. Impact of eIDAS on private sector in general, and on eCommerce in particular, is however, under scrutiny.

eCommerce Europe, that represents 25,000+ companies selling online services in Europe, stated in [48] [47] that "while the eIDAS legislation, which is to be implemented into national legislation by 29 September 2018, legislates for the cross-border recognition of national eID schemes for government services, there are currently no provisions for cross-border acceptance by the industry. This means that while governments and government services across the EU have to accept electronic IDs from another Member State, online

merchants may continue to refuse them." This association noted that only 15% of consumers shop online from another EU country, and advocates boosting consumer trust through a pan-European Trustmark. It also warns about complicated checkout processes requiring too many steps, problems with third party service payments, and need for interoperable e-mandate to facilitate SEPA (single Euro payment area) direct debits.

Business sector analysts have also suggested that mobile payments and commerce will grow exponentially. From the perspective of introduction of mobile vID and biometrics which are also key value propositions of ARIES, the attraction for eCommerce service providers lies with three benefits scenarios:

1. Monetary gain from accessing new consumers (e.g. customers unwilling or unable to use traditional logins or epayments on mobiles devices, but potentially more willing to provide a fingerprint or voice to pay for an order, also accessing cross-border customers thanks to eIDAS support for cross-border recognition of notified eIDs)
2. Business transformation by enhancing the user experience (e.g. using voice recognition, like Siri, Alexa etc to buy on the go, using biometric data to make recommendations depending on the mood or age)
3. Cost saving for cybersecurity operations – secure eIDs are helping create a safer and potentially more trustworthy means and are preventive measures that provide additional security against fraud, therefore reducing the overall cost for detection, recovery and other operational cybersecurity costs.

A recent study [12] says that transaction abandonment rate for eCommerce shoppers using mobile phones outpaces the rate for shoppers using personal computers, laptops, and tablets. One of the main reasons stated for this was that it was too complex to load user ID and credit card information into the system during checkout while using their mobile phone. This limitation means that systems wishing to grant secured access to mobile users need to find elegant ways to authenticate users quickly, without compromising system security, which basically means that different shopping items might need different level of identity assurance, for example depending on the risk or item price.

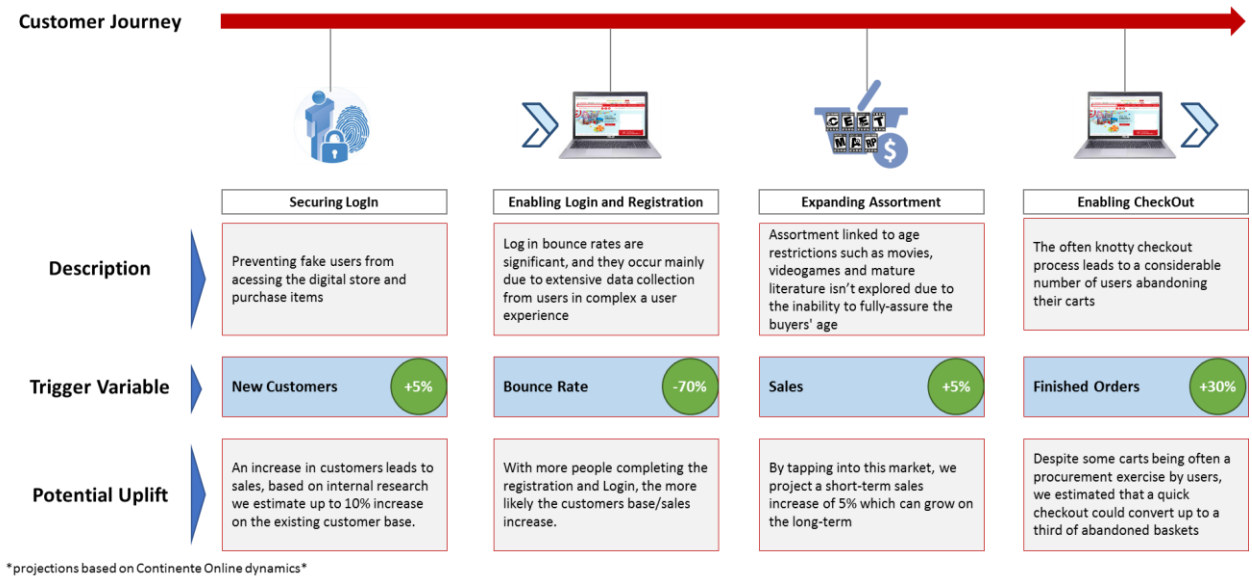


Figure 12: Sonae prediction of benefits from ARIES

In figure 12 we present the first analysis done by Sonae regarding the expected benefits along the customer journey. Projections are based on Continente (brand of Sonae supermarkets) datasets.

In regard to geographical differences, the 2017 CIGI-IPSOS [5]report on online shopping amply illustrates how the likelihood of people shopping online or making mobile payments ARIES by country significantly. In the EU, trust in making e-payments in Poland (65%) or Sweden (64%) was over twice as high as in Germany (27%).

[5] https://www.cigionline.org/internet-survey

The second benefit scenario (use of biometric data to personalise offerings) has many legal and ethical issues, which are already mentioned in D2.2. This deliverable was mentioning Alibaba and KFC system based on a 3-D camera then scans the customer's face to verify their identity and an additional phone number verification option is available for added security. Ver-ID system [47] claims that eCommerce providers could achieve more than 400% return on investments (ROI calculated with data from the following sources: Target, Comscore, Forrester, IBM) if they adopt their solution to “reduce fraud, protect your customers, convert more shoppers”. It helps retailers increase shopper security online and reduces abandoned digital shopping carts by making it easy to log in to shopper accounts. Some commerce chains are launching facial recognition technology to store and tie together data from its store shoppers, online shoppers and loyalty programs. Even the market leader, Amazon, was announcing for some time a way to eliminate fraud by including a verification step, basically taking the selfie with liveliness detection (smile, wink etc). While this plan seems to be put on hold, the physical store named Amazon Go did open up to the public in Seattle in January 2018. The store allows shoppers to pick their items and leave without checking out by using the Amazon Go app, which automatically charges customers’ Amazon accounts for store items. Amazon has not shared details on the methods involved in its "Just Walk Out" technology, but it is likely linked to face detection or image-processing technology.

The third benefit scenario is more straightforward and is not raising any ethical or privacy issues. The cost-effectiveness and cost-efficiency of cybersecurity investments is becoming one of the key priorities for eCommerce operators. As already mentioned, cyber threat is not only about monetary loss, but also reputational damage or attack on brand images, with fake reviews, sentiments and comments. Many brands or retailers invest in operational services to monitor social media. Erosion of trust is further consequence difficult to quantify. In cybersecurity world it is often stated that “prevention is the best cure”, and the investment in preventive measures, such as elevating the level of identity assurance, is increasingly seen as a type of necessary investment. As e-commerce operators move towards mobile channel they face reality that authentication based on passwords only or on social identity is not sufficient for certain types of transactions. In response, alternative authentication mechanisms, including biometrics and two factor authentication are increasingly used. While many e-commerce sites can already detect brute-force logins and suspend, lock, or close potentially fraudulent accounts, this should be measured in terms of cost-efficiency (mid and long term cost, including operational costs, availability etc) rather than cost-effectiveness. Device fingerprinting and risk-based authentication to detect compromised devices and behavioral biometrics to alert them to hijacked accounts are also increasingly used. E-commerce sites also have options of integration with fraud management vendors and could extend it to monitor and detect potential fraudulent transactions. The secure eCommerce scenario in ARIES is focused on demonstrating how virtual identities with different levels of assurance can be used to access different online services and how this level of assurance may determine the operations that peoples are allowed to perform. This scenario will also demonstrate the effective control of citizens over their virtual identities, allowing them to enrol with the ARIES ecosystem and build separate identities, for different purposes, effectively minimizing the disclosure of data and maximizing their privacy.

eCommerce service providers that need to identify and authenticate users have several options. One is to deploy and operate their own identity management system, either licensed off the shelf solution or tailor made e.g. based on some of the open source IAM (identity and access management) solutions. Another one, much more frequent when it comes to e-services for consumers, is the use of external e-ID services and integration of these through so called “identity APIs”. Finally there is also a new subsegment of solutions, commonly addressed as “consumer” IAM or CIAM that are sometimes operated by identity brokers. In the early days of eCommerce, many businesses have first tried to scale internal solutions for external identity management purposes, but capturing, protecting and leveraging highly scalable customer identity data requires huge investment, so that later they migrated or decided to integrate external e-ID services. Reuse of the existing e-ID, such as social network login, is today by far the most convenient option, preferred by the most eCommerce providers.

The Google OpenID API lets third-party web sites and applications let visitors sign in using their Google user accounts that uses OpenID standard. Google also offers other APIs such as web authentication of Google client authentication, for web-based applications, that allows the application to access a Google service protected

by a user's Google account. The Facebook connect API enables login using the Facebook account, as well as the ability to request and display some additional Facebook account information. The Keystone Identity Service is API that allows clients to obtain tokens that can be used to access OpenStack cloud services. The Identity Link API returns data associated with reputation management, fraud reduction, and machine learning management. In principle Touch ID from Apple could also be included in this category of social login solutions. These are only few example of identity APIs that reduce time and cost for application or online service developers.

Implementing social login might be good for bridging the gap between usability and security, but it fails when it comes to high level of identity assurance, even the main players, such Facebook and Google improved their security features with multi-factor authentication, remote logout and unauthorized activity detection. The main problem with these solutions remains the first step: self-enrollment without any strong identity proof, such as government issued e-ID. There are also concerns about what private information they're giving up when they use social login. When it comes to use of social login by mobile apps, Facebook authorization, for example, can ask for up to 40 different permissions, ranging from access to photos to list of friends and more. It is up to the mobile app developer to decide which ones are required for a particular app, and which ones are optional, but expect one or two they all require review by Facebook before the app is published.

Facebook has consistently made gains as an identity provider and in Q4 2014, the social network again held onto the majority of logins and surpassed the 60% share, having in mind all types of online service providers). The company made particularly strong gains in regard to authentication services on mobile devices and mobile eCommerce although, as figure 13 shows, its market share among eCommerce providers dropped 2%

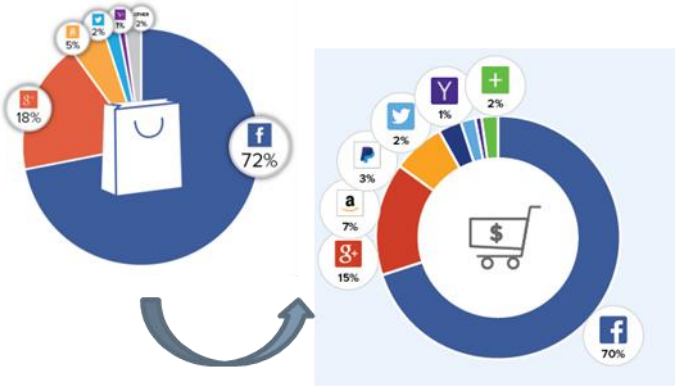


Figure 13: Shares of social login use among eCommerce providers from 2014 to 2016 (based on data from Gigya)

This market share, which is about 10% higher for eCommerce adopters than for the other online service providers, is probably due to the identity attributes Facebook account shares with service providers, which fits into the "analytics-driven" picture of e-identity from the figure 11. Early in 2014, Facebook announced new approach to controls for Facebook Login, allowing users to choose which pieces of profile data they want to allow websites and apps to access upon logging in. This and other efforts to increase transparency and understanding about how user data is handled, show that new opportunities for privacy-preserving e-identities are emerging. In addition, actions against fake accounts are increased. As reported in [49] Facebook shut down 583m fake accounts on the site in the first three months of 2018.

Besides direct integration of external e-ID services through the identity provider available APIs, e-service providers have also an option to use broker or aggregator of different identity providers that might offer additional functionalities, such as proxy to mobile devices, protection of consumer privacy and processing some data. One example is Gigya which has been recently bought by SAP. Other competitors include LoginRadius, Microsoft Azure AD, Janrain, Ping, Social Annex, Addshoppers, Ubisecure, Okta or OneAll. These

solutions are sometimes called Identity clouds or CIAM (customer identity and access management) solutions. CIAM claims many measurable benefits and return on investment, such as 20-30% more efficient marketing & sales, reduction of the abandonment rate during the registration (that can be as high as 70%), or savings through simplified and unified infrastructure. The business model of CIAM vendors is based on charge per user or per transaction and implementation usually takes from 4 to 6 weeks. For e-service provider there is no large investment since identity is provided from the cloud and support is given by CIAM operators. There are also API management and API gateways integrated with identity management solutions. CA Identity Portfolio for example comprises many solutions such as Identity Management and Governance, Privileged Access Management, Single Sign-On, Advanced Authentication, and Directory products. The product can be deployed on-premise, but also as SaaS through partners. For authentication, CA Identity Portfolio includes social logins, KBA, and OTP (email, phone, and SMS). Third party authenticators interoperate with the platform while API gateway provides set of features for mobile scenarios, including device-to-back-end API authentication, device-level certificate management, single sign-on to multiple apps, and the ability to transfer user sessions across devices. Similar to direct integration of social logins, there are new opportunities on the horizon for privacy-aware or privacy preserving solutions. With the General Data Protection Regulation (GDPR) coming into effect in May 2018, many other e-ID providers, including the leading CIAM vendors such as Janrain or Evidon, have released GDPR-ready solutions. SAP, which is the leading EU software vendor with the strong presence in retails sector, bought CIAM vendor Gigya to extend its Hybris offering into the customer identity and access management (CIAM) market. Many market analyst saw this motivated by “GDPR consideration, given that Gigya has not yet released any GDPR-specific solutions and SAP is EU based company”.

More recently identity verification APIs for eCommerce providers appeared on the market and their adoption is very fast, especially on mobile devices. One example is Socure's ID+ solution that includes a series of modular offerings via a single API to validate consumer's identity data through correlation of the identity across 300+ certified offline, online and social data sources as well as provide predictions on the authenticity (whether the identity is real or not) and fraud risk of the individual. A different approach is taken in AriadNEXT’s facial recognition API service, which is comparing selfie taken by mobile phone with picture from eID card. Trulioo’s electronic identity verification (eIDV) platform, Global Gateway, and related API is another example aiming to automate ID checks and reduce integration time. Going back to Facebook as the favourite social login for mobile and eCommerce, in January 2018 it has been confirmed that it had acquired Confirm.io [50] , Boston based startup that offers an API that let other companies quickly verify users government-issued identification card. With 60 employees and about 4 M dollars turnover, it is relatively small company (comparable to IDology or AuthenticID). Much larger Jumio [26] , is now regularily featured in news and market reports. This includes 2018 issued Gartner “Market Guide for Identity Proofing and Corroboration” [51] which names Jumio “representative vendor” for the new sub-segment that Gartner names “identity corroboration”. Whether this brand new (as of May 2018) term will be accepted, it still remains open.

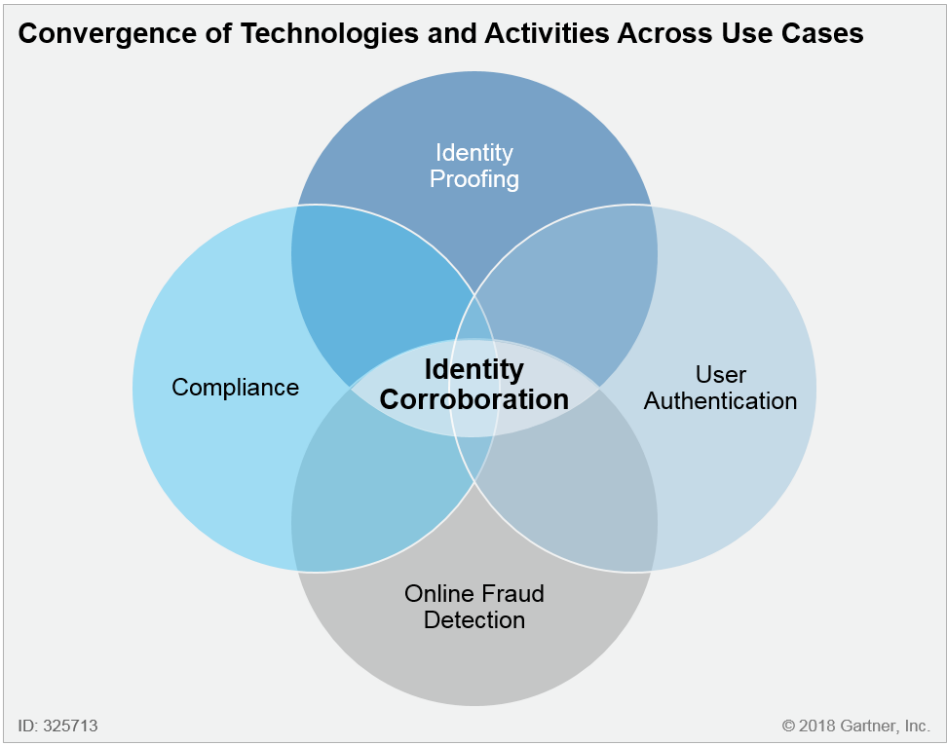


Figure 14: Identity corroboration, as defined by Gartner

Corraboration (to support with evidence or authority, to make more certain) is in this definition (see figure 14) referring to a subset of identity proofing and verification (IPV), but as already stated elsewhere in this deliverable, the naming of emerging segments (including words "proofing" and "verification") is far from being coherent.

Among early adopters of "corroboration" or IPV technologies among eCommerce providers we can mention Instacard whose example could also drive ARIES business case. Instacart is one of the top new eCommerce companies with a $3.4 billion dollars evaluation. Its customers can mix items from multiple stores into one order and have it delivered by a personal shopper. Since it is a kind of "community shopping experience", new Instacart shoppers go through a self-guided identity verification process as part of the onboarding process. These include picture of their government-issued ID, with their smartphone, as well as a selfie, together with liveliness detection, to make sure the shopper featured in the selfie is the same person featured on the e-ID card.

In the next version of this deliverable we will present more details from Sonae business case (figure 12) and will get more data about user experience as the main driver for e-ID adoption in eCommerce. The success of eCommerce depends on removing friction at every step along the customer journey, but also on prevention of data breaches, and paying more attention to privacy requirements and legal obligations. Adding complicated authentication steps to the customer journey in an attempt to improve security is not an option for eCommerce providers where competition is very tough. Fraud control cannot impact consumer experience, while data collection should not endanger trust relationship. Is this all possible, is still to be seen.

6.2 *Smart Airport*

„Smart Airport", is a concept defined in different ways by different people, but it is always involving use of new technologies in service of passenger's services, or economical and security elements of the airport operators

and other stakeholders. In ARIES vision, the list of these stakeholders, normally not analysed in smart airport concept, is also including law enforcement authorities (LEA).

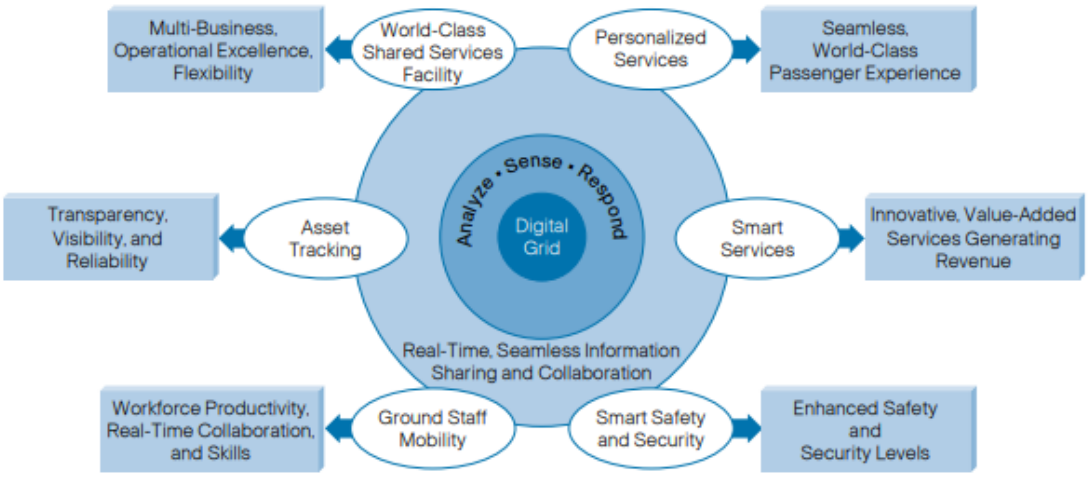


Figure 15: Smart airport vision from Cisco in 2009 [53]

In Cisco vision from 2009 [53] , airports evolve into "virtual service providers" (VSPs) that offer an integrated value proposition for different customer segments. Similar visions were published in other papers, e.g. WIPRO [54] . Airport IT Systems that could be potentially affected by these new technologies include Terminal Operations Management Systems, Slot Allocation Management Systems, Ground Handling Management System, and others, and technologies brought in connection with the concept usually rely on some sort of sensors, which is more recently tagged as "internet of things" domain of application, similar to e.g. Smart City or Smart Stadium concepts. In ARIES, however, we limit our attention to a specific part of this vision, namely reconciliation between improved passenger experience with enhanced safety and security. The main points raised by dissatisfied passengers are usually matched by solutions such as seamless self-services with no waiting time, real time event notifications, on-demand contextual info delivery etc.

In a matter of fact, self-service is already present today throughout the passenger journey, from online check-in, bag drop, security & boarder control and even boarding gate. This already sets high standard for passenger experience: travellers are being able to choose the moment to check-in, and to better manage his/her own time, for example by having time in the entertainment and dutyfree area.

The whole process could be broken down into several steps, from the online ticket purchase, online check-in and issuance of the boarding card, its verification at security and customs control, to the boarding gate checks.

From privacy perspective, linkage of an individual travel document eID to other behaviour and transactions by an individual in the airport (e.g. Duty Free shop) is more accepted in the society. Airlines from some states, however, see identity data as commercially privileged data that they own the moment the individual buys a ticket. Mining that data to sell the individual some product (like another holiday) may be commonplace and not seen as overly intrusive. However, targeted advertising might raise ethical considerations, as it was already noted in D2.2. Another perspective to be taken into account is law enforcement perspective and the support for LEA. While crime related to the online ticket purchasing is the same like in the eCommerce use case, the identity fraud in the other steps has not only financial consequences, but is linked as well as national security, critical infrastructure protection etc.

Besides "identity verification", another distinction of ARIES, compared to the overall smart airport concept, is the central role of mobile phones. According to the SITA [55] , almost 98 percent of passengers carry at least one mobile device while traveling. However, 46% of air travellers still prefer face-to-face check-ins and is not doing online or mobile check-in. When it comes to IT solutions, some airlines use ready-made solutions for online check-ins provided by Amadeus, SITA, and others, while others develop their custom apps to accelerate boarding. As of 2017, online check-ins through apps is behind those through websites (and printing physically

boarding pass). It has also been reported in [55] that passengers say that if an airline or airport application has a bag-tracking feature, they would install it. AirlineCheckins.com launched by Lufthansa Innovation Hub, is another approach to digitalizing check-ins. It is an automated check-in assistant that checks in travellers all over the world for flights on 190 different airlines [56] .

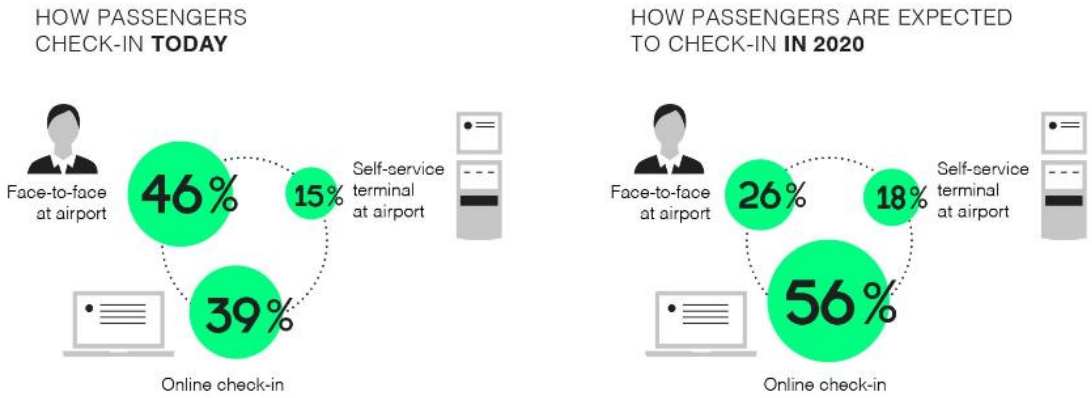


Figure 16: How passengers check in today and in 2020 (Source: SITA 2017)

The Travel & Mobility Tech Radar by Lufthansa Innovation Hub [57] reported that this new way of check-in already has 850 users.

The next identity verification point is at security and customs/border control checks. For many intra-EU flights there is only boarding pass check, so this step became optional for many flights. The main trend here, in the international context, is automated passport control kiosks. These are provided by large technical vendors in the industry, such as IATA Timatic Solutions that can be integrated with most check-in and booking systems. While passengers scan their documents for the flight, the airport system combines their personal and itinerary data and transfers it to AutoCheck. The AutoCheck database contains information about regulations and recommendations for passport information, visas, health papers, airport taxes, currency and customs regulations, which are all necessary for passport control.

Finally, there is identity verification at the boarding gate, done by airline staff. Airlines started also to experiment with biometric verification. In the beginning of 2017, for example, JetBlue announced the implementation of a facial recognition system, supported by SITA software.

These two trends of evolution of the smart airport identity verification systems, namely at border control and at boarding gates, should be analysed separately from different perspectives. Main goal of both trends is to shorten the time spent by each traveller on the identity verifications and to make it more convenient, but the drivers, constraint, legal framework and many other issues are different. As the need to protect European borders and enforce better control of immigration rises there are additional trends in border control that may impact ARIES as well. Nevertheless, the extensive analysis of trends related to border control is not the main scope and we will focus on the use of vID for the boarding but also for the other smart airport services (duty free shop, parking, luggage deposit etc)

The typical self-service gate provides reading of passport (both graphical and electrical) and in more advanced cases also visa verification. Current offer of self-check-in nonetheless contains gates with a camera with facial recognition capabilities and also a possibility to issue digital tokens for supplied mobile App. The concept of the seamless boarding has been proposed by IATA as One ID [58] . In case biometry is used the biometric data (face) is stored on server side of the system, used for all subsequent verifications and deleted after the passenger has boarded the plane or after defined retention period. The document verification is always a part of the boarding pass issuance and the system usually does not rely on a pre-enrolled identity used for higher number of flights. In less frequent cases such as UAE wallet App the user may be able to virtualize his whole

travel information (ID document, visa and boarding pass) in order to user highly streamlined process combining both border automated border control and boarding, but in this case the solution relies on server stored information and the App contains references to the data on server only [59] .

The backend systems processing the boarding pass data are largely based on legacy applications but the newly offered solutions are usually designed according to “privacy by design” approach such as Orchestra by VisionBox [60] .

As mentioned before, the boarding gate automation use case is inevitably linked with automated border control technology and there are strong integration trends. There are several plans how to make the airport scenario seamless: to secure the whole process by biometric data and store the whole information on server side. The user would enrol to the system with his biometric data, the enrolment would create his identity in the system strongly bound to his facial features. The airport flows would rely on biometric recognition at specific check points. The system would scan the face of the user, recognize him and verify he is eligible to move on in the process. There are plans the recognition would be done ubiquitously without any specific checkpoints or gates. The backend information may be stored in classical way with extra protection of privacy based on segregation of duties, but there are also plans to use more advanced technologies such as Blockchain.

The link between the boarding and border control means the backend systems would store information about the passenger travels and requests of border crossing which may provide more security. The last user’s country would be known and any unexpected presence would be reported as security incident. In broader terms the systems provide a way how to replace classical solid electronic documents by information stored in cloud and using only user’s biometry as his ID.

The ramp-up of the new solutions is slow and usually done by pilots with smaller steps such as “a secure and innovative seamless experience” pilot at Terminal 4 of Changi Airport [62] launched in 2017 or airline pilots such as British Airways [61] or Lufthansa [63] .

The ARIES project provides a solution close to the first trend: unification of check-in process with secure identity bound with the boarding pass. It has advantage of identity reusability with much better user convenience. The enrolment may be done at home, but unlike the current online check-in where the identity is self-verified (therefore it has the lowest level of assurance), in ARIES the level of assurance (LoA) of the identity is the approximately same as of the one with the enrolment in a controlled environment. The privacy in case of ARIES is provided by design: only limited information is submitted to the system and the submission must be confirmed by the user. The automatization of the boarding process in the same in both cases, but it is constrained by the legal regulations, to be further analysed in WP2. The systems are capable of automated operation with limited number of operators dedicated for example to incident resolution.

Note that even though the ARIES has only a limited advancement in the boarding scenario in comparison to similar pilots, it provides much better user experience and privacy preservation, especially in the case of other smart airport services such as duty free shopping where the user has much better control over privacy and the system may provide fully anonymous information.

The comparison with the border control use cases is difficult. Because of the legal implications ARIES does not have ambition to be a full replacement of current border control solutions. The trend of virtualization of user identity and usage of cloud, explained in supply side analysis chapter, instead of electronic document is in clear contradiction with the privacy preserving principles. The user would be identified many times and even though the system may be well protected from the external attacks the threat of insider attack or fraudulent processing by government organizations may heavily impact user acceptance.

Figure 17: Typical airport traveling experience with identity verification checkpoints

The identity virtualization scenario in ARIES Smart Airport pilot is starting around the time this deliverable is to be submitted, so there are no exact figures or details about costs or benefits. It will focus on the process of issuing and linking virtual identities with their physical counterparts, clearly establishing their level of assurance and how they can be further derived into convenient and privacy-preserving "pseudo-identities". Both, the virtual identity derivation process and its usage for physical and digital authentication purposes will be linked to citizens' biometrics, minimizing the chances of identity fraud, through the introduction of secure vault. The use and access to the security vault by LEAs officers where all enrolment and identity derivation is stored during the enrolment phase is of crucial importance. This vault, properly described in deliverable D3.1 will store, properly protected, biometric features from opting-in citizens from countries enrolled in ARIES ecosystem, which can be checked by LEAs under specific circumstances (e.g. credential issuing process, criminal investigations) and accessed and used by data subjects following the forthcoming General Data Protection Regulation.

On another front, pilot will also examine privacy benefits from the passenger point of view, since the boarding pass or identity documents usually contains more information that what is really needed for the control purposes (e.g. full name, date of birth, flight time and destination, etc.). ARIES self-derived identities can be used to provide a higher level of privacy by just presenting a proof of having a boarding pass, without need to disclose any other personal data.

Another set of activities related to Smart Airport pilot will be interlinking with the other stakeholders. While two airlines already confirmed their interest to become associated partners in ARIES, a number of other stakeholders will be approached. IATA and ICAO, for example, are studying how to improve the current situation. The ICAO Technical Advisory Group on the Traveller Identification Programme's (TAG/TRIP) New Technologies Working Group (NTWG), is addressing enhanced use of the ePassport., while IATA PEMG is working to revisit the E2E passenger journey, including the promotion and development of self-service options that rely on mobile technology and the capture of both biographic and biometric data. To support these efforts, the PEMG has four sub-groups working on: 1) Biometrics; 2) Common Use; 3) Fast Travel; and 4) Passenger Facilitation. Within IATA, the developing One Identity initiative is exploring the concept of a single travel token, most likely based on biometrics, which can be used both for industry processes and government requirements. Other groups that work in relevant standardisation might be contacted in coordination with WP6, for example ISO SC17 WG10. IATA mobile ID working group was starting in 2017, while National Institute of Standards and Technology (NIST) in USA also started activities around Digital driver's license.

6.3 *Other uses*

In chapter 3.3.2 it was already mentioned that the vID can be used in different contexts and for different purposes. The selling proposition related to co-existence of several different vIDs on a single mobile device, is

making it possible to have different levels of assurance, privacy preferences or even usage policies, linked to each one of vIDs derived from the same government-issued identity document. Therefore we can talk about context-sensitive usage of vIDs, as one of the main value propositions, should also be seen in the light of authentication to online services, mobiles apps or other devices. In [13] GSMA study, which is reproduced in table 13 in this deliverable, we can see that users expect almost any access control, both physical and online, as well as many privacy-sensitive applications, such as e-voting, to be linked with mobile phone.

In a matter of fact Mobile ID authentication together with NFC compliant phones is already used also for physical access. In [8] several examples from educational sector were presented, for example access control in Villanova University, the University of San Francisco, and Arizona State University. To open locked doors, participants present the phone to a door reader, just as they would a student ID card. In Europe there are also several experiments in educational sector. In [64] even mobile ID cost benefits analysis was presented with Aarhus University's comparison to the current identification and access control system. The immediate benefits include reduction in the cost creating and distributing student ID cards, as it is assumed students who own a smartphone will prefer to use the mobile ID.

In fact, authentication and physical access control created new market segment, so called mobile-based keyless technology solutions. The hospitality industry, also known as "tourism and leisure industry" is a broad category of fields within the service industry that includes lodging, event planning, theme parks, and many others. One of the associated partners in ARIES is Lopesan, that owns a chain of hotels in Canarian Islands and it is especially interesting target sector for ARIES. Another related market is rent a car or the market for unlocking delivery boxes (post office, logistics etc).

OpenKey is a hospitality technology startup that helps hotels offer mobile room keys to guests, although based on Bluetooth technology for access control. The other similar vendors are Zaplox, Iris, Proxce and others, mainly relying on Bluetooth and not linked to verification of government issued ID.

The first pilot with NFC mobile key [65] took place in Stockholm in 2013, while the comparison between these two technologies for "smart room access" was done in 206 with the conclusion that "it makes economic sense for hotels to adopt NFC access control solutions" [66] . However, rather than use of mobile keys for pure physical access control, ARIES vID are more likely to be used in a combined cyber-physical scenario, maybe in combination with storage of additional attributes, such as loyalty points, discounts, homeland security requests etc.

With the emergence of sharing economy and in particular AirBNB or similar portals, there are new challenges to guest registration that can be extended to any shared access to private assets. Location relevant attributes of a guest, driver, or passenger, could also be part of vID used for the access control.

While hospitality industry might be the right target for physical access control, financial sector, and especially payment industry is already adopting IPV solutions very fast, due to the strict new anti-money laundering (AML) and know your customer (KYC) regulations, requiring them to verify the identities of all their users. Increases in synthetic and fraud identities and new cross-border account opening are another driver. The European Union AML directive regulation states: "Accurate identification and verification of data of natural and legal persons is essential for fighting money laundering or terrorist financing. Latest technical developments in the digitalization of transactions and payments enable a secure remote or electronic identification." It is not surprise that mobile payment is opening door for many other sectors. In 2015 Mastercard has rolled out Identity Check Mobile, that uses biometrics like fingerprints or facial recognition to verify a cardholder's identity to simplify online shopping. Amazon applied in 2016 for a patent application for a system that would allow users to authenticate themselves with a selfie or video to complete a transaction, something that is already used in several solutions available on the market. Android Pay also uses NFC to transmit card information to the retailer's point of sales POS device. Unlike ARIES, Android Pay uses tokenization and HCE to store card information securely. Samsung Pay is similar and it uses NFC as well as a fingerprint or a PIN. Apple Pay is a kind of hybrid approach that uses both NFC and a tokenization, but also requires the consumer to enroll using biometrics. Consumers then register their credit or debit cards in the Apple Wallet as a one-time registration and payment tokens are stored securely in the secure element on the iPhone device. Owners of well-known in-app payment solutions (e.g. Uber) are maybe another target audience for ARIES.

Governmental and healthcare sectors are also natural targets for ARIES. e-Prescription for example, is the process of issuing a prescription by a medical doctor, ordering medicine by the pharmacy, pickup by the patient and reimbursement by the insurance that in theory can be done, at least partially, through the mobile phone and with vID services for authentication or authorization. Digital documents can be signed electronically, they can be delivered in a specific mobile mailbox, notification receipt can be signed etc. even e-voting can be more secure and user-friendly. Estonian solution claims to save "800 working years" and on during the elections [67] about 30% of voters logs onto the system using an ID-card or Mobile-ID, and casts a ballot. The voter's identity is removed from the ballot before it reaches the National Electoral Commission for counting, thereby ensuring anonymity. With ARIES there are even more elegant ways to implement it.

Finally, although it was briefly mentioned in e-Commerce scenario, the cyber-physical use of vID, for example to extend attributes with loyalty card points, can also be seen as an opportunity for ARIES.

7 *Exploitation Plans*

As we have seen from the previous chapters, different types of identity ecosystem already exist, with many inter-related stakeholders. In some countries, like Switzerland, Germany Sweden, Denmark or Norway, consolidation and partnerships are on the way with the role of government reduced to recognition, regulation, and control and monitoring. This model is broadly in line with vision of ARIES ecosystem, but it is also true that the virtual ID provider under the current legislation is not clear. It could be trusted service provider, but in the future it could also become "notified ID", as defined by eIDAS regulation. While legal and ethical opportunities and threats are discussed in WP2, here we will complete strengths, weakness, opportunities and threats (SWOT) analysis with findings from market analysis. In addition we present several alternatives business models and the first outcomes of the joint exploitation discussions, with the assets clearly identified and ownership assigned to individual partners.

7.1 *SWOT analysis*

A market analysis, as well as legal and socio-ethical analysis from the work package WP2, delivers some insights into opportunities and threats for ARIES project results, while strengths and weakness are collected from technical value propositions in other work packages, user validations and partners individual plans and positioning. All of these suggested inputs have been debated in a collaborative session during the project meeting organised in March 2018 in Prague at Gemalto premises.

A comprehensive SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis is therefore not limited to technical features vis-à-vis other identity services in the selected market segments, but is also looking into global and specific positioning of results, having into account selling propositions or existing network of contacts.

	SUMMARY
Strengths	Speed and ease for customers
	Elevation of level of assurance increases confidence and trust among stakeholders
	Decreases risk of breaking the law (e.g. selling specific goods to under-aged customers) due to the improved use of derived credentials and attributes
	Strong consortium with experienced and well-known industrial partners
Weakness	Dependent on consumer hardware/device
	Deployment is complex
	Cost of related services e.g. integration, may be too high
	IPR and licensing is fragmented
Opportunities	Digital onboarding of a new segment of customers (e.g. elderly, cross-border or those that have trust issues regarding current authentication technology)
	Possibility of consumer profiling and segmentation, according to the consumer selected vID, privacy and trust levels
	Increasing demand for strong customer authentication due to the compliance requirments
	Increased importance and visibility of cybersecurity risks, where ID theft is recognised as the main threat
Threats	The system integration and ARIES platform configuration might become obsolete rapidly
	Legal constraints and changes within the area of eIDs variable according to the location and not yet fully understood
	There is still some reluctance and uncertainty over the use of biometrics
	Competitive solutions for e-identity proofing and verification already exist
	Need for certification and/or accreditation

Table 4: SWOT Analysis

In the table 4 we can see that some of value propositions and selling arguments from this deliverable were not taken into account during the SWOT brainwriting session. This is due to the fact that the timing of this exercise was parallel to the writing of this deliverable. The summarised list of findings will be presented to the project partners at the next project meeting in order to validate this initial SWOT analysis and the results with their feedback will be presented in the final version of deliverable D5.2.

7.2 *Business model analysis*

Understanding of the commercial incentives and drivers for consumption of identities and attributes is still not clear beyond the obvious incentives for service providers like targeted advertising (for free identities provided by social network and likes that share user data with service providers). Identity as an enabler or service is often provided in the context of an established agreement, government issued ID or federation Id in education, while identity as business is more common to corporate world where technology providers sell solutions to organisations for employee ID management.

Balance between the monetary and the non-monetary value of personal data is open issue and behavioural economics behind privacy is still not mature enough to bring valid alternatives to existing online identity business models.

The following business models are under consideration at the moment:

7.2.1 Identity Proofing and Verification-as-a-Service

In this business model am IPV service provider builds out a SaaS-mode set of services that could include identity proofing and verification. This business model for ARIES partners can be based on selling technology or even providing services to the third party. The service provider charges their business customer for this SaaS service through a subscription to the service. Early examples of this model are companies that work for credit or banking companies including LexisNexis or Experian, but with the emergence of remote biometric verification technologies, there is a whole new bunch of IPV-as-a-service providers, such as already mentioned in chapter 5.2.1. Business opportunity for ARIES is related to the target audience such as sector-specific organisations with the capacity to operate identity proofing and verification (IPV) with clear service level agreements, 24x7 supports etc. We can distinguish between existing IPVaaS providers and the new ones. Business set-up for ARIES exploitation starts with an offering that would include a subset of technical result (e.g. modules needed for verification) and additional services, such as training, maintainance, cloud storage etc. In this business setting, most of the revenue would go to ARIES technology and service providers. The service might even include full operation of IPVaaS in case some of ARIES partners decide to make additional investment in building full support team. In any case, according to generic ARIES exploitation strategy and agreements, specific % of the overall revenue would go to IP owners.

7.2.2 Selling technology and services

In this business model, the external entity (target customers range from existing identity providers to different service providers or sectorial umbrella organisations and associations) becomes a trusted identity manager of a consumer's identity information. ARIES project partners are limited to the selling of product (software) or services (e.g. system integration, deployment, maintenance). The identity data is owned by the consumer, but the identity provider could either charge to the consumer for any identity service (issuance etc.), or can have an agreement with the consumer that their identity will be given to the third party that needs that identity information. In this model, the consumer (in theory) could be "paid" for usage of their identity, but the revenue model will depend on the API used by identity provider. In the case of existing popular third party identity providers such as Facebook or Google ID, actual revenue comes indirectly, from generating more traffic, therefore being more attractive to potential advertisers.

In the ARIES meeting in Prague it has been agreed not to use term "Identity provider" to refer to organisations that operate eDNI or ePassport scheme, which should be addressed as trusted document issuer. ARIES targets specific subset of identity providers that would become "Virtual ID Provider", which can be the same organisation that also carries out the biometric verification, although it can be also a separated entity. In addition some service providers could be interested in technology, for example for the in-app identity management.

7.2.3 Identity Brokers

The Identity Broker business model is based on the existence of a middleman to connect those who offer (identity providers) and use (service providers) identity attributes. However, the revenue model is different and instead of charging the consumer for identity management services, or charging the service provider subscription, identity brokers might apply different pricing schemes per transaction, relationship, level of assurance offered/used etc. Examples are brokers that enhance identity provider offering, additional to Google or Facebook ID. There is a growing demand from service provider that use Google or Facebook ID API to have also more trustworthy information about the user, such as the user's street address or whether they were authenticated with something stronger than a password (Authentication as an Attribute). Since popular

consumer identity providers are generally not considered trustworthy sources of these attributes, other companies like postal and mobile operators, or even education institutions are better positioned as "attribute providers." Another innovation in identity data business model are data cooperatives that operate kind of anonymized identity data "lake".

Business opportunity for ARIES lies in the targeting brokers that work with several online service providers, as well as attribute providers (e.g. education, healthcare, post, some public administrations, bank etc). The attributes retrieved from them could be used for building additional virtual ID different from the one derived from e-ID or ePassport, therefore enhancing or complementing ARIES. Business set-up is slightly different since these stakeholders need to be considered as potential technology customers (brokers) and partners (attribute providers). This is probably the most complex situation as additional software is needed to be integrated with ARIES platform and value chain is extended, but in terms of future opportunities it could prove to have high return on investment.

7.3 *Joint exploitation plans*

A successful commercial exploitation of the ARIES technology will require close co-operation of all parties providing IP, other products and services. The elaboration of joint exploitation plans is following two side approach: from bottom-up (collecting and analyzing individual exploitation plans) and top-down (presented here). In the final version of deliverable (D5.2), after trade-off analysis is done and feedback is received, the appropriate actions will be presented. It is already clear (see annex 1) that some partners are in the process of transformation (e.g. Idemia) or merge and acquisitions (e.g. Gemalto). In addition Smart Airport pilot did not take place yet, so many open issues remain.

In some of the above mentioned business models, there is the potential integration of, as yet, unidentified providers of alternative technology components into an 'ARIES' solution, so the meaning or branding of ARIES needs to be carefully considered.

What has been already suggested, however, is that prior to the commercial launch of the ARIES service, all ARIES participants will need to reach a contractual agreement covering the following topics:

- Commercial responsibilities of each party including inter-country commercial account management (e.g. lead generator, sales and contract manager)
- An indicative business model and pricing of each component of the ARIES service (e.g. license based with range of prices)
- The percentage revenue split due to each party (IP owners, Lead Generators and Service Providers) which will depend on the mix of product, services and Lead Generation responsibility. These parameters are likely to vary with each client contract. Revenue will be a mix of capital sale and annuity revenue for licenses and services.
- The responsibility for the provision of consultancy – may be client dependent.
- The responsibility for System integration, deployment, support – these will likely be dependent on territory.

It is also possible to make several different agreements that treat these issues separately, for example a joint exploitation agreement that covers framework for the further commercialization that can be implemented through specific partner group agreements (among two or more partners).

The 'value proposition' to the end customer needs to be clearly defined before the selling proposition and an indicative price is defined. Each IP owner should define license (open source or proprietary), business models (provision as a service, license based etc.), cost and pricing strategy etc.

There is already strong commercial competition in the e-identity market segment, as presented in this deliverable, and therefore the unique selling proposition (USP) of ARIES over these offerings needs to be

considered and clearly stated as a competitive analysis. This will be an ongoing responsibility of different technology owners.

The flexible and modular nature of the ARIES architecture enables substitution of individual components with the others, either off the shelf or to be developed for the specific customer. Spanish eID verification, for example, can be replaced with a different component that uses different technology for French eID, which currently does not have electronic data, or even UK eID which is not linked to specific unique ID number of ID card.

The end user pricing will take several factors into account. These include:

- Cost of marketing/sales
- IP holders pricing for their element of the solution (which should be described and estimated per element in the annex of the final exploitation plan)
- Services (defined in the paragraph below)
- Acceptable profit margins to all involved parties

When it comes to Marketing & Sales management, it is likely that commercial opportunities will arise through

a) existing IP holder's client relationships,

b) lead generation by non-IP holders e.g. ATOS and SAHER or

c) demand from potential users not related to any of the ARIES IP partners.

On the other hand, IP owners can be expected to market/sell ARIES through their normal channels as part of their usual business practice. The Lead Generation and contract managers in each of these scenarios need to be determined and clearly defined to all ARIES parties. Where an IP holder is the Lead Generator then they would be expected to make presentations and demonstrations where required. Where the Lead Generator is another party (not IP holder) then the account ownership, contract management, budget ownership of providing the pre-sales support needs to be determined. The party agreed to be the commercial lead for a particular sales Lead will be responsible for account management and client contract negotiation. There is a strong element of client HQ territory priority when assigning account management responsibility for logistical and linguistic reasons.

7.4 *IPR and licencing*

During the last months of 2017 and the start of 2018, the intellectual property (IP) ownership map of ARIES components was discussed, in case those partners want to protect their rights or license their components.

The ARIES platform and a number of components will also be made open source and distributed under open source licenses, to facilitate a wide adoption of the project outcomes in the European ICT security, cloud and big data ecosystems, and to maximise their impact. The project is considering the publication of certain outcomes under appropriate open source licenses (e.g. EUPL, LGPL, etc.) to be determined by Consortium partners.

components	Ownership
ID proofing service	IDEMIA
Biometric enrolment service	IDEMIA
Enrolment Web Application	GEMALTO
ARIES Secure Vault service	IDEMIA
Virtual Identity Issuer based on Idemix	UMU
Mobile ID issuer	GEMALTO
vID Verifier service based on Idemix	UMU
Mobile ID verifiifier	GEMALTO
Biometric Verifier service	IDEMIA
Spanish eDNI Verifier	ATOS
ePassport Verifier and ID proofing client	IDEMIA
Biometric Enrolment client	IDEMIA
Mobile ID Issuance Manager	GEMALTO
Issuance Manager as Idemix recepient	UMU
Mobile ID Authentication client	GEMALTO
vID Authentication client based on Idemix prover	UMU
Biometric Authentication client	IDEMIA
Secure Wallet	GEMALTO
Credential Manager	ATOS
Idenity selector	UMU
Integration APIs	All

Table 5: IP ownership of ARIES components

7.5 *Organisation of Future Activities and Sustainability*

As a starting point, a preliminary list of important factors has been considered for ARIES sustainability, containing:

- Policy recommendations
- Contacting privacy communities and discussing post-GDPR privacy challenges
- Analysis of trust relationships/frameworks and building partnerships with relevant organisations
- Proactive addressing of commercialization barriers i.e. material for user training and support
- Continuity of ARIES infrastructural components after termination of the project;
- Maintenance of other project results (common specs, APIs);
- Clarify composed (multi-stakeholder) business models for the different stakeholders
- Business case factsheets and other material justifying further investments;
- Coordination and agreements among partners;

- Actions related to the existing communities of interests
- Identify and fund a few “first deployment” applications

The short term actions are related to the validation of assumptions raised in this deliverable, such as provisional SWOT table, business models, reconciliation between individual and the joint exploitation plans, etc. Specific actions will be taken in relation to the associated partner group and specific interest groups, including a newsletter with summary of this deliverable. Dissemination and communication actions will be more focused with market-oriented messages and results positioning. Finally, we will also pose market perspective for the project results validation, including the validation of technology readiness level (TRL).

Is the ARIES result ready for the market?	***Recommendations***
1.1 Is there a document with solutions architecture, use case and link to business case?	Take use cases from ARIES and collect cost/benefit data from users in order to transfer these into business cases.
1.2 Are technical specifications based on standards?	Explore situation and opportunities together with WP6. Contact different communities.
1.3 Is the result modular, open and able to integrate with potential existing solutions (incl. from other vendors)?	Invite other industrial partners to join interest groups and provide feedback.
1.4 Are there any legal/regulatory barriers for market adoption?	Explore situation together with WP2.
1.5 Are there any manuals, reference implementation and implementation guidelines?	Involve associated partners in validation of these materials.

Table 6: Market perspective for results readiness

8 Conclusion

ARIES is a project that has many specific challenges and characteristics. Setting up of a reliable identity ecosystem in itself is a very big challenge and ARIES objective is to provide the technical platform, as well as the first group of stakeholders for it, but the full identity ecosystem is very difficult to establish, as it was witnessed by analysis of several existing examples in this deliverable. The starting point is likely linked to an existing sector, such as eCommerce, or cross-sectorial scenario, such as Smart Airport. However, trust, as the key enabler, should be already present, either through the previous identity service relationships, or through strong set of legal and organisational guarantees, as well as accepted set of rules and standards; in other words, ecosystem is inexorably linked to trust framework. ARIES is integrating many new technologies, processes and

security features, with the existing ones. The overall result is rather innovative, but at the same time there is sufficient architectural modularity and functional flexibility in order to make distinct combination and "flavours" of ARIES results. The market impact challenge is therefore addressed through this "lego" strategy where individual results, owned by different intellectual property owners, can be assembled "on the run" and provided either directly by the owners, or through sales channels, including consulting and system integration companies.

Several goals might have been looking as contradictory in the past, for example privacy-respecting virtual identity management processes with the traceability needed to achieve a reduction in levels of identity fraud. However, recent technical, but also societal and legal trends (e.g. awareness about importance of privacy, general data protection regulation – GDPR etc.) make ARIES exploitation not only feasible, but also likely to happen. With all this, ease of adoption and convenience for all end-users are not sacrificed, although this needs to be validated during the final phase of the project. This last phase should therefore, also address validation of economic impact and realistic scenarios that allows building a solid business case with sufficient data for return on investment (ROI), as well as the first deployment references.

Based in the preliminary findings, the offering of ARIES for different stakeholders can be defined as:

- An integration package allowing service providers to include secure e-ID services of all end users holding a virtual eID.
- Documentation and support for the service providers in order to assure an easy set-up and running of the service.
- Easy to use, trustworthy and understandable user interfaces to make use of e-ID services such as authentication
- Enhanced control of the e-ID data for citizen, that is able to decide elements of their identity data to share, while letting other stakeholders such as service providers and LEA, to have sufficient data for their needs, such as service provision or combating ID theft.

ARIES ecosystem needs further alignment with existing initiatives and trends, such as Connecting Europe Facility (CEF), built around its core service platform of Digital Service Infrastructures. While eIDAS, GDPR or NIS directive, as well as AML4 or PSD2 directives, are creating important opportunities for ARIES, the new proposal for a regulation on strengthening the security of identity cards in EU, should be specifically addressed in the rest of the project. Other ethical, socio-economic, technological and organisational aspects of identity solutions, as well as identity-related crimes should also be reviewed for the final version of this deliverable.

Two scenarios, eCommerce and Smart Airport are very different and the ARIES platforms, resulting from an adaptation of ARIES system and specific components, might have different exploitation strategy and roadmaps. In this deliverable we have explored trends on both demand and supply side after looking more closely at these two uses of vID. The findings need to be incorporated into the packaging strategy, as well as marketing material needed for the last phase of the project. While the list of components and IP ownership in this deliverable was based on the preliminary list taken from the system architecture document in month 8, the continuous updates were needed in order to reflect dynamicity of the project situation. It is likely that the list of components needs to be revisited once again before the project ends.

The next big milestone is related to Smart Airport pilot. The automation of some steps, like identity verification, might find constraints when designing the technical solution, as well as combating the use of fraud (e.g. barcodes on the boarding pass can be forged). Virtual identities should be validated e.g. to present proof of having a boarding pass and certain attributes, in a privacy-respectful manner, without the need to disclose any other personal data. Special attention should be paid to validation of risks, e.g. risk of biometrics data leakage.

	Proofing	Issuance	Management
Assurance	Government issued eID/ePassport, biometrics, multi-factor AuthN		Storage in secure wallet, accountability through secure vaults
Usability	Mobile v-ID with simple and intuitive apps		
Privacy		Derived privacy-preserving attribute based credentials	Decentralization

Table 7: mapping demand side priorities to technology trends

Besides packaging of project results and validation of exploitation assumptions in the smart airport scenario, the remaining effort in WP5 will also be spent on fine tuning of ARIES positioning, both on demand and supply side. In table 7, we try to summarise the main areas of focus, those where ARIES has identified value proposition and could build strong and possibly unique selling proposition. Need for higher assurance is obvious on demand side, and it has been met by many different solutions, from strengthening of proof (e.g. smart card based e-ID) to multi-factor authentication. While ARIES is not unique in this space, the fact that it also matches the demand for privacy –preserving e-ID does make it rather rare among commercial solutions matching both demands. Solution based on government issued physical e-ID or ePassports, that has decentralised management functions, with support at the same time for secure v-ID storage managed by user, as well as derivation log traces in secure vault accessible to LEAs, is another strong selling argument. This pair of "value propositions" (table 7), rather than a single value proposition in itself, is what makes ARIES unique and should be further explored also for selling purposes.

The final version of deliverable should also explore tension between different stakeholder priorities. For example service providers might request more attributes than actually needed, which is a concern for the user privacy. Trade-off situations and a variety of alternative technical solutions and future trends might enhance final market analysis report.

9 References

[1] Guillermo Jimenez, Nathalie Galeano, Teresa Najera, Jose Manuel Aguirre, Ciprian Rodriguez, Arturo Molina, METHODOLOGY FOR BUSINESS MODEL DEFINITION OF COLLABORATIVE NETWORKED ORGANIZATIONS, Part of the IFIP — The International Federation for Information Processing book series (IFIPAICT, volume 186)

[2] Daniel Fields, Ownership and governance models in collaborative IT projects – Atos whitepaper, https://es.scribd.com/document/110190223/WHITEPAPER-Ownership-and-Governance-Models-in-Collaborative-IT-Projects-V10-Oct-2012

[3] Alessandro Acquisti, various papers, https://www.heinz.cmu.edu/~acquisti/

[4] EU report Bringing down barriers to unlock online opportunities, https://ec.europa.eu/commission/priorities/digital-single-market_en

[5] Federal Trade Commission report, March 2017, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

[6] Forrester study: Top Trends That Will Shape CIAM In 2018 And Beyond, http://www1.janrain.com/rs/253-XLD-026/images/top-trends-that-will-shape-ciam-in-2018-and-beyond-industry-research.pdf

[7] UK government Good Practice Guide No. 45, Identity Proofing and Verification of an Individual, Sept 2015, https://www.ncsc.gov.uk/content/files/guidance_files/GPG%2045%20%20-%20validating%20and%20Verifying%20the%20identity%20of%20an%20individual%20-%20issue%202.4%20-%20NCSC%20Web.pdf

[8] Secure technology Alliance, Mobile Identity Authentication, March 2017 https://www.securetechalliance.org/wp-content/uploads/Mobile-Identity-Authentication-WP-FINAL-March-2017.pdf

[9] NIST Special Publication 800-63-3 Digital Identity Guidelines https://pages.nist.gov/800-63-3/sp800-63-3.html

[10] Guidance for the application of the levels of assurance which support the eIDAS Regulation, EC document

[11] Fly to Gate, The Biometric Airport Journey, Gemalto brochure

[12] “7 reasons why customers are abandoning your mobile shopping cart,” Ventureburn, January 18, 2016, http://ventureburn.com/2016/01/7-reasons-why-customers-are-abandoning-your-mobile-shopping-cart/

[13] Mobile Connect, Mobile Connect Consumer Research Report: United States, http://www.gsma.com/personaldata/wpcontent/uploads/2015/10/mc_us_paper3_10_15.pdf.

[14] e-identity solutions in Estonia, https://e-estonia.com/solutions/e-identity/smart-id

[15] My Identity App (MIA) website, https://www.mia.at/en/

[16] open eCard initative, https://www.openecard.org/en/startpage/

[17] German e-ID client webpage, http://www.der-eid-client.de/

[18] Trust Frameworks for Identity Systems, http://www.openidentityexchange.org/wp-content/uploads/2017/06/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

[19] Developing Trust Frameworks to Support Identity Federations, January 2018, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf

[20] National Strategy for Trusted Identities in Cyberspace – Enhancing Online Choice, Efficiency, Security, and Privacy, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[21] FutureID project, http://www.futureid.eu/

[22] Ponemon study, Global Trends in Identity Governance & Access Management, https://www.ponemon.org/news-2/74

[23] Ariadnext facial recognition service, https://www.ariadnext.com/products/idcheck-io/

[24] Authada IPV services, https://authada.de/

[25] Chekk offering, http://chekk.me/consumers/

[26] Jumio ID verification, https://www.jumio.com/

[27] Mobile Connect, GSMA introduction, https://www.gsma.com/identity/mobile-connect

[28] Verimi platform, https://verimi.de/en/

[29] Acuity The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy, https://www.acuity-mi.com/GBMRIntroPreview.pdf

[30] J. Camenisch and A. Lysyanskaya, "An efficient system for non- transferable anonymous credentials with optional anonymity revocation," in Advances in cryptology-EUROCRYPT 2001, pp. 93–118, Springer, Berlin, Germany.

[31] J. Camenisch and E. V. Herreweghen, "Design and implementa- tion of the idemix anonymous credential system," in Proceedings of the 9th ACM Conference on Computer and Communications Security CCS '02, pp. 21–30, ACM, New York, NY, USA, November 2002.

[32] C. Paquin and G. Zaverucha, "U-prove cryptographic specifica- tion v1.1," Tech. Rep., Microsoft, New Mexico, NM, USA, 2011.

[33] A. Sabouri, I. Krontiris, and K. Rannenberg, "Attribute-based credentials for trust (ABC4Trust)," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 7449, pp. 218-219, 2012.

[34] Primelife project, http://primelife.ercim.eu/

[35] IRMA project, https://privacybydesign.foundation/irma-en/

[36] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S.Kumar, and K. Wehrle, "Security challenges in the IP-based Internet of Things," Wireless Personal Communications, vol. 61, no. 3, pp. 527–542, 2011.

[37] Jose Luis Canovas Sanchez, Jorge Bernal Bernabe and Antonio F. Skarmeta, "Integration of Anonymous Credential Systems in IoT constrained environments", in IEEE Access, vol. 6, pp 4767 - 4778, 2018.

[38] Jorge Bernal Bernabe, Jose L. Hernandez-Ramos, and Antonio F. Skarmeta Gomez, "Holistic Privacy-Preserving Identity Management System for the Internet of Things", Mobile Information Systems, vol. 2017, Article ID 6384186, 20 pages, 2017.

[39] Tobin, A.; Reed, D. The Inevitable Rise of Self-Sovereign Identity. The Sovrin Foundation 2016

[40] ALASTRIA project, https://alastria.io

[41] Uport webpage, https://www.uport.me/

[42] Jolocom webpage, https://jolocom.com/

[43] Evernym webpage, https://www.evernym.com/

[44] Mitek webpage, https://www.miteksystems.com/mobile-verify

[45] Kofax webpage, https://www.kofax.com/products/mobile-capture/mobile-id-and-verification/features

[46] Economist Intelligence Unit, Digital identity authentication in e-commerce, https://www.identrust.com/pdf/EIU_IdenTrust_Digital_Auth.pdf, 2007

[47] Ver-ID webpage, http://appliedrecognition.com/ecommerce

[48] eCommerce Europe, Opportunities and challenges for the e-commerce sector, https://www.ecommerce-europe.eu/news-item/long-read-e-identification-rise-opportunities-challenges-e-commerce-sector/

[49] News about Facebook closing accounts in 2018, https://www.theguardian.com/technology/2018/may/15/facebook-closed-583m-fake-accounts-in-first-three-months-of-2018

[50] Facebook buys Conrim.io, https://www.confirm.io/

[51] Gartner report "Market Guide for Identity Proofing and Corroboration", https://www.gartner.com/doc/3872992/market-guide-identity-proofing-corroboration

[52] Secure Digital Transactions Kitemark, https://www.bsigroup.com/en-GB/kitemark/services/secure-digital-transactions/

[53] CISCO white paper, Smart Airports: Transforming Passenger Experience To Thrive in the New Economy, https://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf

[54] WIPRO white paper, Intelligent airpots, your runaway to success http://www.wipro.com/documents/intelligent-airportsyour-runway-to-success.pdf

[55] SITA Passengers IT Trends Survey, June 2017, http://www.sita.aero/globalassets/docs/surveys--reports/passenger-it-trends-survey-2017.pdf

[56] Lufthansa Innovation Hub, https://lh-innovationhub.de/en/project/airlinecheckins/

[57] Medium website of LIH, https://medium.com/lufthansa-innovation-hub

[58] OneID concept paper, https://www.iata.org/whatwedo/passenger/Documents/OneID_Concept_Paper-Version1-January2018.pdf

[59] Gulfnews article, Now, smartphone is your passport in Dubai, https://gulfnews.com/news/uae/emergencies/now-smartphone-is-your-passport-in-dubai-1.2040149

[60] International airport review article: Passenger Data Privacy: there is one traveler identity management Platform Certified in Privacy by Design. That is Orchestra, https://www.internationalairportreview.com/news/68937/passenger-data-privacy-there-is-one-traveler-identity-management-platform-certified-in-privacy-by-design-that-is-orchestra/

[61] Findbiometrics article, British Airways Lauds Success, Expansion of Biometric Boarding Trials with CBP, https://findbiometrics.com/british-airways-biometric-boarding-trial-expansion-503092/

[62] Changi airport website, A seamless digital experience through One Changi ID, http://www.changiairport.com/corporate/media-centre/resources/publication/changi-journeys/issue-7/a-seamless-digital-experience-through-one-changi-id.html

[63] Digital trends article, Board 350 passengers in 20 minutes? Facial recognition passes testing at LAX, https://www.digitaltrends.com/photography/lufthansa-self-boarding-gates-biometrics/

[64] Mobile authentication with NFC enabled smartphones, Technical report ECE-TR-14, Aarhus University, http://eng.au.dk/fileadmin/DJF/ENG/PDF-filer/Tekniske_rapporter/samlet-ECE-TC-14.pdf

[65] Evaluation of the world's first pilot using NFC phones for check-in and hotel room keys, https://www.assaabloy.com/Global/Products/Products-old/ASSA-ABLOY-Mobile-Keys/Report-ASSA-ABLOY-Mobile-Keys-Pilot-Clarion.pdf

[66] Smart guestroom entry: BLE or NFC?, https://www.asmag.com/showpost/19819.aspx

[67] e-Governance and i-Voting in Estonia, webpage, https://e-estonia.com/solutions/e-governance/i-voting/