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

ARIES
"reliAble euRopean Identity EcoSystem"

D2.3 – Legal requirements and analysis of ID legislation and law enforcement aspects

Due date of deliverable: 31/08/2017
Actual submission date: 24/08/2017

Grant agreement number: 700085
Start date of project: 1 September 2016
Revision 2.3

Lead beneficiary : UMU
Duration: 30 months

Project co-funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020	
Dissemination Level	
PU = Public, fully open, e.g. web	✓
CO = Confidential, restricted under conditions set out in Model Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC.	
Int = Internal Working Document	

D2.3 – Legal requirements and analysis of ID legislation and law enforcement aspects

Contributors
Nacho Alamillo (UMU) and Julián Valero (UMU)

Reviewers
Dave Fortune (SAHER) and David Martin (GTO)

23-08-2017
Revision 2.3

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
1.0	12/05/2017	Nacho Alamillo (UMU) Julián Valero (UMU)	First draft version
1.1	18/07/2017	Nacho Alamillo (UMU) Julián Valero (UMU)	Incorporation of eID requirements and LEA Access requirements
1.2	05/08/2017	Nacho Alamillo (UMU) Julián Valero (UMU)	Incorporation of EU eID legislation detailed analysis Version submitted to ethical advisor
2.0	14/08/2017	Nacho Alamillo (UMU) Julián Valero (UMU)	Version submitted for editing revision
2.1	21/08/2017	Nacho Alamillo (UMU) Julián Valero (UMU)	Review
2.2	22/08/2017	Nacho Alamillo (UMU) Julián Valero (UMU)	Review
2.3	23/08/2017	Nacho Alamillo (UMU) Julián Valero (UMU)	Final review

Executive Summary

This document aims to analyse the legal context and requirement that apply to the ARIES service ecosystem, including:

- An analysis of the eID European Union legislation, and its application to the ARIES ecosystem, mainly focused in the Regulation (EU) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (commonly known as "eIDAS Regulation") and its implementing acts.

  Our findings include that an ARIES provider may play two different roles in the eID EU regulated ecosystem:

  - First of all, an ARIES provider may be an electronic identification means consumer. This happens when the ARIES provider uses the electronic identification means issued to the citizen i.e. by the Member State, such when the citizen authenticates using a national citizen ID card (i.e. the Spanish National ID card, or the German nPA).

  - Secondly, an ARIES provider may be an electronic identification means issuer, in the sense of the eIDAS Regulation. For this to happen, the system must comply with the legal requirements set forth by the eIDAS Regulation, and the corresponding implementing acts, and be recognized by a Member State.

    The ARIES derived identities aim to be recognized according to the substantial security level defined in Article 8 of the eIDAS Regulation and, thus, the system shall comply with the corresponding requirements set forth in the eIDAS Security Regulation.

- An analysis of the use of advanced electronic signatures based in qualified certificates issued by ARIES providers, a legal institution also mainly regulated in the eIDAS Regulation.

  Our finding include that an ARIES provider may play two different roles under the concept of trust services:

  - An ARIES provider may issue qualified certificates assuring the identity of the person, using pseudonym certificates and other attributes, as a means to represent derived identities. This possibility is directly implementable in the current EU framework, but its recognition is subject to the authorisation of the usage of pseudonym certificates in each Member State.

  - An ARIES provider could offer a new trust service, consisting on the accreditation of possession of personal attributes (a wide conceptualization of identity) with privacy protection. This may be considered as the main legal innovation of the project: an ARIES provider, once a person identity has been provisioned, provides a service that allow 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 constitute assertions that may legally substitute 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.

To be able to substitute these documents per partial derived ARIES identities, maintaining legal certainty, we shall propose the definition of this services a new trust service, defining the service and a legal effect attained to the service (i.e. establishing some sort of equivalence principle such as "where the law requires the documental accreditation of a personal attribute, it will be possible to use a [service name] evidence".

Thus, the implementation of this possibility, which will be further analysed during the rest of the project, it will be needed to adopt it as a new trust service, ideally at the EU level, or at the Member State level (a more realistic scenario).

- An analysis of the personal data protection issues and of the law enforcement access to evidential information aspects, mainly according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

- A briefing on other legal requirements that are relevant to the ARIES project, regarding the information society and consumer regulations.

The document is completed with a bibliography section and an annex with the detailed list of the relevant legal requirements identified in the study.

Contents

List of figures

1 Introduction

1.1 *Purpose of the document*

The main goal of the document is to identify the legal implications related to the ARIES providers operating in the ARIES ecosystem.

The scope includes the following areas:

- An analysis of the eID European Union legislation, and its application to the ARIES ecosystem, mainly focused in the Regulation (EU) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (commonly known as "eIDAS Regulation") and its implementing acts.

- An analysis of the use of advanced electronic signatures based in qualified certificates issued by ARIES providers, a legal institution also mainly regulated in the eIDAS Regulation.

- An analysis of the personal data protection issues and of the law enforcement access to evidential information aspects, mainly according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

- A briefing on other legal requirements which are relevant to the ARIES project, regarding the information society services and consumer regulations.

1.2 *Relation to other project works*

Functional requirements of the ARIES ecosystem are defined by WP2 in D2.1. Technical design of the ARIES ecosystem is defined by WP3 in D3.1.
The document is a deliverable of WP2 and it will be used as input for the development of W2.4 – privacy and data protection compliance. It will also be used as input for the WP demonstrators, regarding the legal aspects of both pilots.

1.3 *Structure of the document*

The document is structured as follows:

- **Chapter 2** provides an overview of the ARIES technical ecosystem and its actors, from a legal perspective.
- **Chapter 3** provides an analysis of the eID European Union legislation, and its application to the ARIES ecosystem.
- **Chapter 4** provides an analysis regarding the use of advanced electronic signatures based on qualified certificates issued by an ARIES provider.

- **Chapter 5** provides an analysis of personal data and law enforcement aspects as applicable to the ARIES ecosystem.
- **Chapter 6** provides an analysis of other legal requirements applicable to ARIES ecosystem participants.

The document also contains a bibliography section, and an Annex with the detailed legal requirements that have been identified.

1.4 *Glossary of terms and acronyms adopted in this document*

eID	Electronic identification means
eIDAS Regulation	Regulation (EU) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Text with EEA relevance).
eIDAS Cooperation Decision	Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)
eIDAS Interoperability Regulation	Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).
eIDAS Security Regulation	Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).
eIDAS Notification Decision	Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (notified under document C(2015) 7369).
Consumer rights Directive	Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council

	and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (Text with EEA relevance).
e-Commerce Directive	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
Law enforcement Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

2 Overview of the ARIES technical ecosystem and its actors, from a legal perspective

The ARIES project main goal is to deliver a comprehensive framework for reliable e-identity ecosystem comprising new technologies, processes and security features that ensure highest levels of quality in eID based on trustworthy security documents and biometrics for highly secure and privacy-respecting physical and virtual identity management, with the specific aim to tangibly achieve a reduction in levels of identity theft, fraud and associated crimes.

The set of solutions are being designed to achieve required levels of multi-party trust with efficiency, ease of adoption and convenience for all end-users (citizens, law enforcement, businesses), consolidating Europe as world leader in enhanced identity based services as a basis to boost the competitiveness of its economy. ARIES leverage virtual and mobile IDs cryptographically derived from strong eID documents in order to prevent identity theft and related crimes in the physical (e.g. an airport) and virtual (e.g eCommerce) domains. Both, the derivation process, and the derived IDs are univocally linked to citizens' biometric features, increasing the level of identity assurance during the credential issuance process and during authentication.

Highest data protection standards will be followed to provide digital privacy-preserving features. Thus, the project will provide a global approach for ID Ecosystem in Europe to address European-specific concerns to improve identity, trust and security, and better support the law enforcement to address the new threats in cybersecurity while achieving far-reaching socio-economic positive impacts.

ARIES will demonstrate its outcomes and the levels of identity prevention reduction achieved in two use case demonstrators (secure eCommerce and identity virtualization for secure travel), covering the complete vision of virtual id ecosystem and its practical application.

According to D3.1, ARIES project is focused on two main use cases: secure eCommerce and identity virtualization for plane boarding control or similar cases that require identity virtualization.

There are several technologies that may be used for implementation and all have comparable security and privacy features: pseudonymous PKI, zero knowledge proof technologies, anonymous credentials. The pseudonymous PKI was selected as a first proof of concept of the project; other technologies may be used in later stages.

2.1 *A technical architectural vision*

The architecture defined for ARIES project follows two main principles: privacy by design when the sensitive information is anonymised and each actor of the system has only very limited visibility on user data, and full accountability: user information is stored in several secure vaults with restricted access and only legal authorities would have the ability to investigate suspicious behaviour.

ARIES system is a set of components responsible for creation of virtual identity tokens, verification of electronic documents and acquisition and verification of biometric data. The architecture is defined in modular way, each component may have a different supplier, the system is fully open and allows interoperability among ARIES and non-ARIES Identity Management systems.

The architecture addresses all the weaknesses identified in the use cases and reaches required level of privacy, the real strength and privacy depends on technology used, pseudonymous PKI was used as a model as it is a typical state-of-the-art approach and even this typical technology provides sufficient level of privacy if the architecture is deployed in the way defined for ARIES project. Also, according to D2.3, the system architecture is depicted on figure 1. Each component is described below.

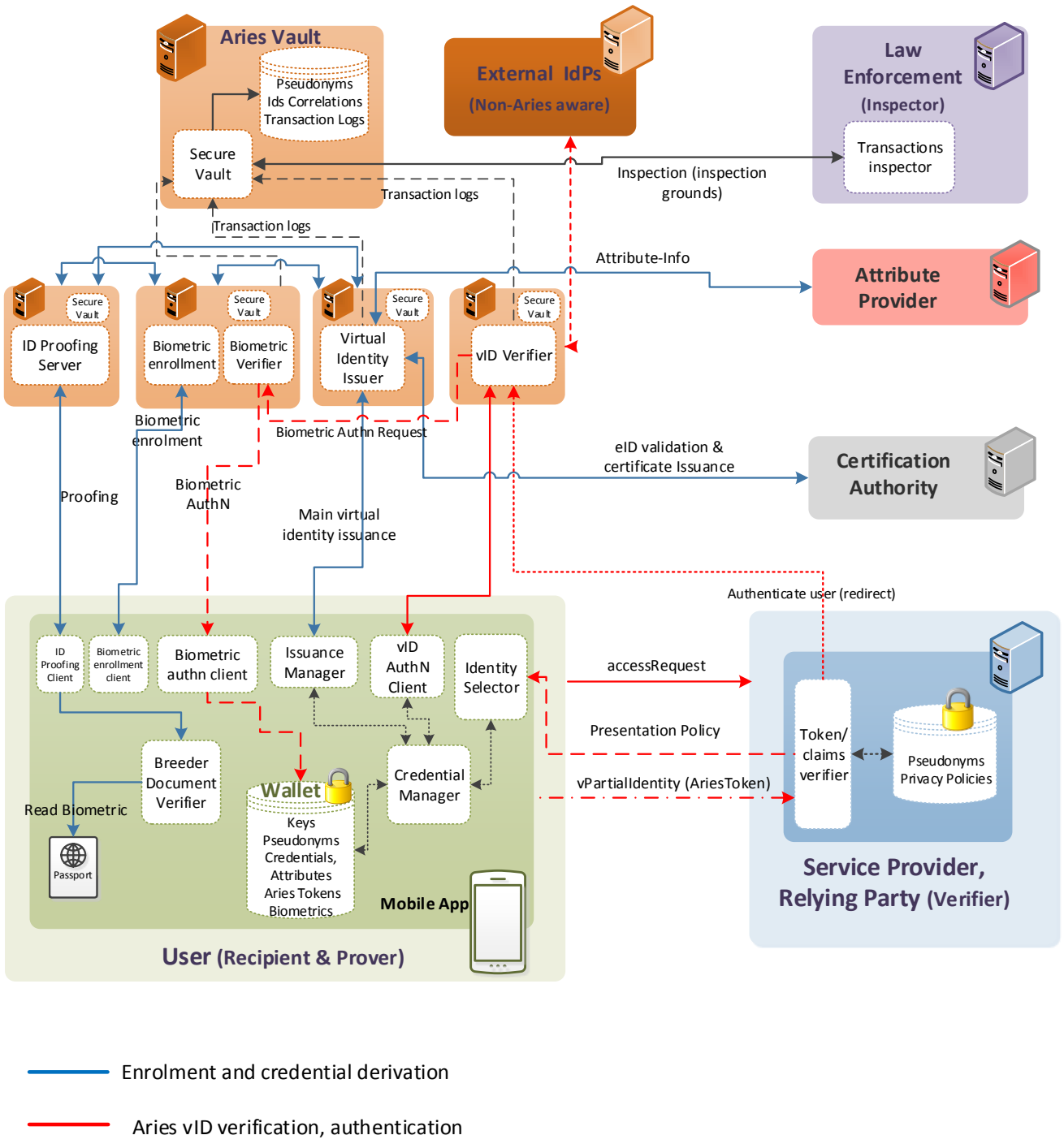

Figure 1 - ARIES Architecture

The components have been aggregated according to the main roles identified in the architecture, that is: IdM services, Service Provider, User, Law Enforcement (inspector), Attribute Providers, Certification Authority. For the sake of clarity, each of these main roles are depicted in the figure in a different colour.

The system is composed of many components and each component may be deployed by a different party. Trust establishment is one of the most important tasks during the deployment. The means of the establishment and technology used is not defined by ARIES project, is left open. The project will rely on typical schemes such as HTTPS authentication or digital signature based technologies (SAML, OpenID Connect):

- **Identity Management Services:** The ARIES ecosystem has been designed to be open and extensible, so that it can consider different identity service implementations for each of the main kind of IdM services supported. Therefore, these services can be offered by a different IdM provider. Nonetheless, in order to enable and set up the ARIES ecosystem, these IdM services need to implement specific requirements such as to enable trust between each other, as will be described throughout this section. In addition, the user service or app will need to incorporate the corresponding libraries to interoperate within the proper IdM service being adopted. The integration among the different services is achieved through the trusted ARIES IdM secure vault that stores the correlations between the different IDs-pseudonyms that user holds across different IdM services. This secure vault is used for auditing the process, enabling future Law Enforcement inspections.

- **USER - Mobile app**. This is the handset app for mobile devices that interacts with the Identity Management services explained above, during the enrolment and vID verification stages. The enrolment part is based on a breeder document (e.g. ePassport) verification and facial recognition of the mobile device owner. This enrolment allows to provision an identifier and credentials (constituting a virtual ID) within a mobile device. Verification part supports two authentication options in push mode: authentication using only vID verification and vID verification with additional biometric authentication.

- **Service Provider (SP)** – it is the Relying Party, one or several web or mobile applications that offer the services as demanded by the scenario use cases, and that rely on the vID Verifier service for authentication. The SP requires specific attributes that will be needed to permit the user access to his service. Nonetheless, the user has the final word, his consent is needed 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 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.

- **Certification Authority (CA):** regular CA that stores, issues and signs the user certificates and provides also revocation information (CRL, OCSP). It is the root trusted entity in which the PKI relies on; trust in the user key relies on the trust in the validity of the CA's key. The component may be used directly for issuance and management of certificates for vID or as a supplementary component for other purposes such as source of trusted ICAO or eIDAS certificates. Note that this component is optional and may be replaced with a different cryptographic application if different scheme that PKI is used.

- **Attribute Provider**: The ARIES ecosystem considers many attribute sources including the ARIES vID itself. The attributes could be provisioned for the vID directly.

- **Law Enforcement Inspector:** this entity is in charge of the inspection of the transaction logs stored in the vault when the inspection grounds are fulfilled. The Inspector role is in charge of de-anonymization of the user and audit log data related to vID usage stored in the ARIES Security Vault in case of identity fraud, misuse, liability or cybercrime investigation. To this aim, the Inspector should satisfy a policy that species which information should be recoverable as well as the circumstances under which the data can be inspected. Notice that this authorization privilege is in the end implemented by providing LEAs with specific cryptographic credentials that allow decryption of such information. Depending on the underneath technology, it might mean providing proxy re-encryption keys or anonymous credentials in case of access to Zero knowledge crypto proofs.

- **External IdPs (non-ARIES aware):** External IdPs, which are not necessarily aware of ARIES technology, 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.

Additional details regarding the ARIES architecture may be found in D3.1 document.

2.2 *Actors and roles in the ARIES ecosystem, from a legal perspective*

From a legal perspective, several actors can take part in the ARIES ecosystem:

- **Identity management service provider**, which is the individual or legal entity that provides electronic identification services to users and service providers, who trust them. Identity management service providers can assume various roles, including the following (extracted from D3.1, section 5.1):

    - **Id Proofing service**: this service has the primary objectives of validating that the user owns a recognized identity. It authenticates the users, remotely checking the validity of its credentials by means of the authentication with the chip included in the bre eder document e.g. ePassport, or eID. The service also checks the consistency between the face picture stored in the chip and a fresh capture of the face image of the user.

    - **Biometric Enrolment service**: this service allows a user to be registered in the system through its biometrics, and therefore, providing a high level of assurance when the user/SPs demand authentication through biometrics to access a particular service.

    - **Enrolment Web Application**: web portal providing a user-friendly interface for the ARIES enrolment process. It allows user to scan a QR code with its smartphone in order to trigger the enrolment process.

    - **ARIES Secure Vault service**: It is a remote service to store evidence collected during enrolment (in particular from the proofing phase). It would offer basic CRUD features (Create, Read, Update, and Delete), for the data stored by a user, and for managing the vaults by an administrator.

    - **Virtual Identity Issuer**: Backend application responsible for provisioning and management of main user Virtual ID (a.k.a. ARIES token). In a first implementation, the ARIES vID is being based on classical PKI digital signature and certificate, so that the issuance service interacts with the Certification Authority, which is the entity that actually generates the x.509 certificates. In the pilot stages of the project the Mobile ID is created relying on Mobile PKI

using as baseline the IP proofing authentication performed previously. Nonetheless, this issuer service may also be implemented by other privacy-preserving technologies such as those introduced in 4.3. 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.

- **vID Verifier service**: This component is in charge of verification of the ARIES vID: the user authentication. When a higher level of assurance is demanded, this service can communicate with the biometric verifier service to request the authentication of the user through biometrics. In case of the traditional approach is adopted, it can perform basic authentication through traditional PKI and using SAML, interacting with the vID Augh client module in the user smartphone. In addition, the vID Verifier service can verify derived partial virtual identities. The approach or implementation for derivation, proving and verification the partial vID is open and can be based, among others, on SAML tokens (attribute-authentication assertions) or by means of ABC-related proofs (cf. section 4.3). For some optional scenarios, this vID Verifier service may be directly deployed in the service provider, so that the user can communicate directly with the SP in a M2M fashion. This approach avoids contacting the external IdM verifier service (managed by a third entity) in every request, which, in turn, avoids the IdM to trace the user's behaviour. The vID Verifier service must trust the Issuance Service; indeed, these two services will be usually managed by the same entity. Besides that, the verifier service must trust the biometric verifier in case this strong authentication is also required during the vID verification.

- **Biometric Verifier service**: This component is in charge of the biometric authentication of the user by interacting with her/him through the smartphone app, to capture a fresh and live biometric image and execute the comparison with biometric reference collected during enrolment. This process is done during the vID verification stage in response to a request coming from the vID Verifier service. It should be noticed, that the verification process requires the user to be beforehand enrolled by the Biometric Enrolment service. In general, these two services are often managed by the same entity. As a result of the biometric verification, a new authentication assertion is sent back to the vID Verifier, during the same session.

Additionally, the identity management service provider may subcontract or delegate some functions to third party providers, such as attribute providers, external IdPs, or trust service providers issuing qualified certificates.

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.

This is especially so when the derived identity is implemented in the form of a qualified electronic certificate for electronic signature, given the liability regime provided in this case by the Regulation.

- **Service provider**, which is the individual or legal entity that relies in the derived identity, typically in a business process, including electronic commerce, electronic government, etc. It may also be the owner of an online platform, such as those used in support of collaborative economy that implements the derived identity to increase security in the relationships between private individuals.

The service provider will be ordinarily a customer of the identity management service provider, or – less likely – a business partner of it, because it is a principal stakeholder regarding the security of its own electronic process.

- **User**, which is the individual person using the identity management services in the electronic relationships that establishes electronically.

3 Analysis of the eID European Union legislation, and its application to the ARIES ecosystem

In the ARIES ecosystem, the use of national identity documents for the electronic identification of the citizen is considered, prior to obtaining a derived identity, according to the procedure indicated in section 4.1.1.1 of D3.1.

For this to be possible, it is necessary to evaluate the regulatory rules of the corresponding national identity document, in order to verify that it does not contain usage restrictions in this regard. In addition, from a cross-border perspective, this means that the identity provider ARIES becomes a party that relies on an electronic identification means notified by a Member State of the European Union, under the terms set out in the Regulation (EU) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS Regulation").

On the other hand, as regards the relationship between the identity provider and the service provider, a derived identity could be considered as a new electronic identification means, which could be accepted by public entities and, eventually private parties, but provided that this mean has been notified by a Member State of the European Union, again under the terms established by the eIDAS Regulation.

It is therefore necessary to examine the content of that Regulation in order to determine the requirements which the ARIES identity management service provider will eventually have to meet.

The European Union regulation of electronic identification is mainly contained in Chapter II of the eIDAS Regulation". This Regulation has been further developed by the following implementing acts, setting rules regarding the electronic identification pan-European scheme:

- Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market ("IDAS Cooperation Decision").

- Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market ("eIDAS Interoperability Regulation").

- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market ("eIDAS Security Regulation").

- Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for

electronic transactions in the internal market (notified under document C (2015) 7369) ("eIDAS Notification Decision").

The eIDAS Regulation consider that "citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States", and also that "mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities" (Recital 9).

According to Recital 12 of eIDAS Regulation, "one of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services", while under Recital 17, "Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions".

Under the eIDAS Regulation, thus, a mutual recognition system is created to allow citizens and business to identify themselves when accessing public services, and also private services if the Member State authorizes this possibility.

3.1 *Legal concept of electronic identification*

According to Article 3 (1) of the eIDAS Regulation, electronic identification means "the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person"; a process which we will see is mainly intended to support the cross-border authentication when accessing public services. This definition is certainly scarce, for which we must turn to other definitions of the same legal text and rely on previously existing self-regulation and on the self-regulation of the public sector created specifically for this institution, especially in the STORK projects and the CEF eID Community.

Article 3 (3) of the eIDAS Regulation defines person identification data as "a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established"; that is, a digital identifier, such as a name, one or two surnames, a registration number assigned by the Government (in the case of Spain, one of the most widely used – in physical identification, but not in remote electronic identification—, is the Document number National Identity). Given the existence of various sets of data that identify a person, and the difficulty of creating a unique identification aggregated with all possible identification data, we will refer generally to partial electronic identities.

So far, electronic identification is a process where we use identifiers of natural or legal persons, but we have not yet established what kind of process is or for what purpose, so we must continue to deepen the analysis of the eIDAS Regulation. Article 3 (4) of the eIDAS Regulation defines an electronic identification scheme as "a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons", while Article 3 (2) clarifies that electronic identification means are "a material and/or immaterial unit containing person identification data and which is used for authentication for an online service".

From these definitions, we can begin to better understanding the concept of electronic identification, since it is characterized by a regime that supports the process of electronic identification by issuing units that contain identification data and that serve for cross-border authentication. This is a legal abstraction that

refers to a large number of potential technologies such as digital certificates in computer applications or cryptographic cards, physical or logical devices that generate unique authentication codes (such as single-use passwords), among many others.

This important amount of electronic identification means, which is available to the Member States, introduces an element of strong diversity between them, both in terms of security and interoperability, hindering or directly preventing cross-border operations.

It is also necessary to note that, according to Article 3 (5) of the eIDAS Regulation, authentication is defined as "an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed". It is very remarkable the fact that this definition refers to three well-known security services: entity authentication, data source authentication and data integrity.

Entity authentication would therefore be the core of the new regulation, since the previous one (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures) sufficiently covered data authentication as well as integrity. It has to be highlighted that the definition includes as well these two other security services: if we compare this definition with that of an electronic stamp contained in Article 3(25) of the eIDAS Regulation itself, we will see that the seal also serves for exactly the same purpose of guaranteeing the origin of the data and the integrity of the same data. And that the advanced electronic seal, in addition, identifies its creator (see Articles 3(26) and 36 (b) of the eIDAS Regulation).

It does not seem, however, that it is obligatory for the electronic identification mean to support all these security services, in view of the use of the "or" conjunction used in the definition, so that we will face identification means that will allow only the authentication of entities – what is commonly perceived as "identification" – while others may also offer the guarantee of data source authentication and even integrity.

On the other hand, for a technology to qualify as an electronic stamp, it is necessary to guarantee the origin and the integrity of the data, so that in some cases this overlap will occur. A similar phenomenon happens with the advanced electronic signature, since it requires the identification of the signatory, the univocal link with the signer, and the possibility of detecting the subsequent modification of the data; that is, entity authentication, data source authentication and data integrity. These services can be technologically based on an electronic identification mean, as defined in the eIDAS Regulation.

That is, in both cases (advanced electronic signature and advanced electronic seal), we will find the possibility that some electronic identification systems offer exactly the same functionalities, as for example in the case of the use of digital signature based on a non-qualified certificate – where applicable, with the support of a cryptographic card – as a means of electronic identification. Indeed, it is clear that technologies such as the digital certificate-based signature can function indistinctly as a means of electronic identification and as a trust service, so we should inquiry the reason why certain technology is designated as an electronic identification mean, a trust service (signature or electronic seal), or both at the same time; and the response can be found in the simple political will of each Member State, that in the exercise of its sovereignty may decide what such system legally is – by virtue of its recognition as such – and even the legal effects that it wishes to give it. And if the only difference is compliance with the conditions of one or another legal regime, this implies that all qualified certificates issued in a Member State, regardless of the ownership of the service, public or private, are potential candidates to be recognized as electronic identification means by that State under eIDAS Regulation.

Taking into account this analysis, the legal regime established by the eIDAS Regulation may be summarized in the following conceptual map:

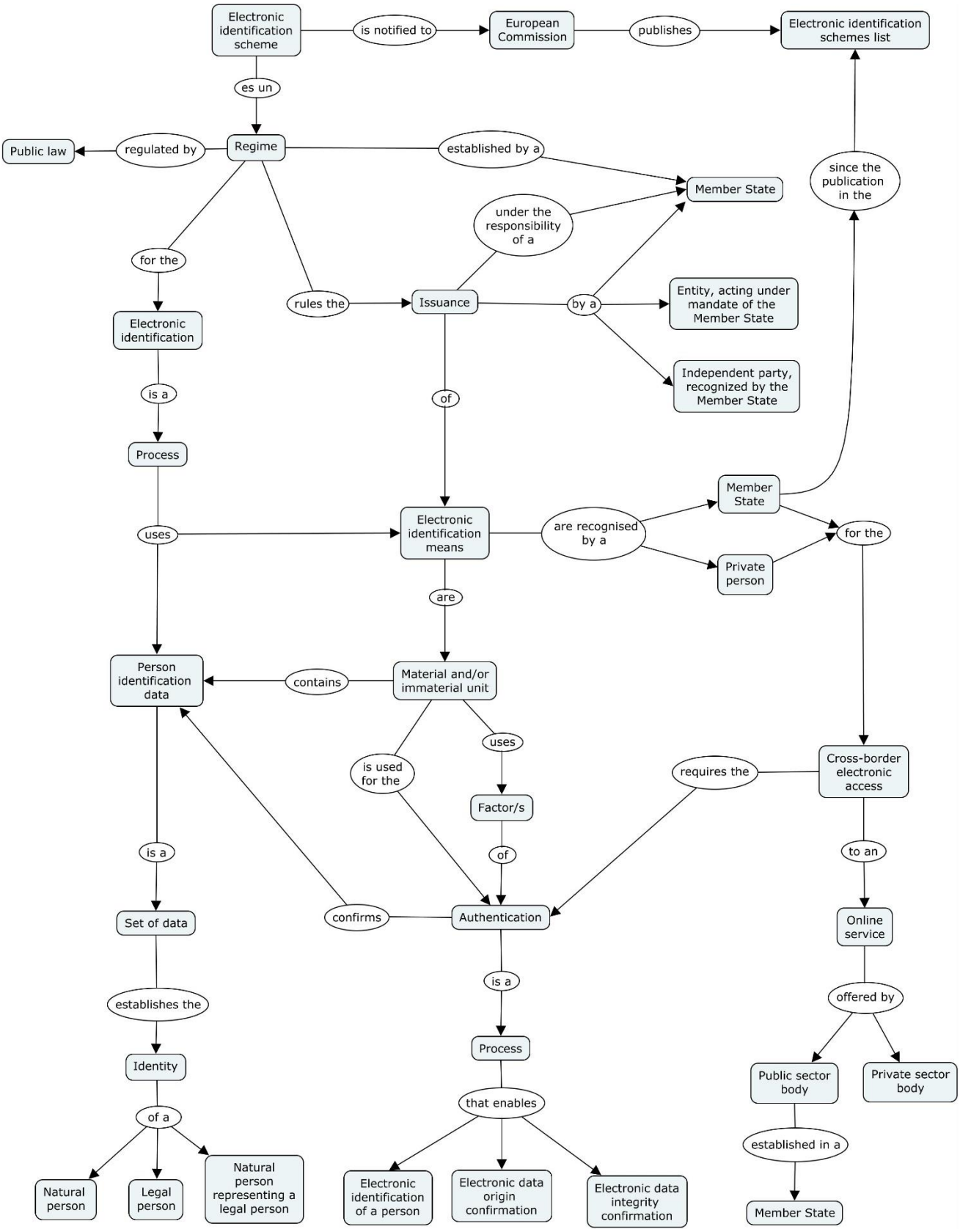

Figure 2 - eIDAS Regulation conceptual map

From a digital single market perspective, it would seem uninteresting for a Member State to confine itself to the issuance of these electronic means of identification, even though they allow authentication of the origin of the data and the integrity of the data. Without that they also comply with what is stipulated to be considered as an advanced or qualified electronic signature or seal; basically, because these systems would not be recognized in the other Member States with the presumptions set out in the Regulation and, therefore, their value would be clearly lower than the technically equivalent trust services.

More common will be, however, the existence of other scenarios of interrelation between the means of electronic identification and trust services. For example, certain means, such as the Spanish electronic DNI, contain a certificate of identity (usable as a means of electronic identification) and, in addition, a qualified electronic signature certificate (trust service, subject to regulation). Another possibility is that the same technical mechanism serves the two functionalities at the same time, in which case it must comply with the regulation provided for electronic identification and for the corresponding trust service, cumulatively.

3.2 *Scope of the Regulation and relationship with national law*

Having presented the concept of electronic identification in the eIDAS Regulation, it is convenient to delimit the scope of the mentioned Regulation, and its relation with the regulation in the national level.

The first thing to be said is that the eIDAS regulation is limited to establishing "the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State" as stipulated in Article 1 (a) thereof, conditions which strongly orbit around the issues of security and interoperability of systems and electronic identification systems and means.

The Regulation is based on a pre-existing reality, which is the identification systems that Member States have in the past established for their citizens, mainly to facilitate access to public services, which were not covered by the electronic signature Directive. Similarly, Recital 12 of the eIDAS Regulation itself clarifies that "the aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible", to facilitate the electronic development of the internal market, to comply with the legal requirements reflected in different legislative instruments, including Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on Internal market and Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, both expressly mentioned in the eIDAS Regulation, and in other instruments of cross-border relationship between citizens and the public sector, such as certain cases in the field of electronic public procurement, electronic invoicing, corporate law or electronic tax management; or even for access to official personal data or for electronic voting.

Ultimately, the eIDAS Regulation is extremely respectful of the competences of the Member States in the area of electronic identification, limiting itself to establishing a framework for the mutual recognition of those systems and to legitimize the provision, by the European executive power, of a European public service. A sign of this respect is that the Regulation "does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States" (Recital 12), which therefore fall within the exclusive competence of the Member States; that "Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services [... and] to decide whether to involve the private sector in the provision of those means" (Recital 13), which again fall within the sphere of exclusive competence of each Member State of the Union.

Finally, Recital 13 of the eIDAS Regulation also states that "Member States should not be obliged to notify their electronic identification schemes to the Commission", and therefore "the choice to notify the Commission of all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States". Thus, it is a regulation with a strong element of voluntary participation by Member States. We can therefore find a second element of diversity between the different Member States of the European Union, including Member States introducing electronic identification systems and notifying them for their cross-border use, against Member States that introduce these electronic identification systems only for internal use.

In fact, from the perspective of the eIDAS Regulation, we can see that electronic identification is a collection of electronic public services, unlike trusted services – of a highly commercial nature – that may be provided under direct or indirect management techniques, although it could also be a private service recognized by the Member State (cf. Article 7 (a) of the eIDAS Regulation), always under its liability. As a result of this model, the eIDAS Regulation will not apply to electronic identification systems provided by public or private entities that have not been recognized by a Member State, which would be outside of its scope. This does not mean that an electronic identification means cannot be issued by the private sector, nor that it doesn't get any recognition, but that this activity is carried out in accordance with national law, or in a self-regulated manner, based on agreements between the parties.

In addition, the eIDAS Regulation does not really constitute the legal basis for the regulation of electronic identification systems, but only for their mutual recognition between the Member States of the European Union. Thus, the true regulation will be found, where appropriate, in the national level. Certainly, the freedom that each Member State will have to regulate its electronic identification system or systems will be conditioned by the rules of the eIDAS Regulation, because compliance with them is a condition for such mutual recognition, so that its effectiveness as a regulatory instrument it's undeniable.

Finally, it should be noted that the analysis of the eIDAS Regulation clearly shows that its provisions only apply to online authentication, which would exclude face-to-face authentication, a fact which is relevant from the perspective of the free movement of persons physically traveling to the territory of another Member State.

From the perspective of the substantive legal effects of the electronic identification systems to which we have just referred, the eIDAS Regulation focuses precisely on their mutual recognition within the territorial scope of application of the regulation, extending the right of use of such systems to the rest of the Member States of the European Union. Thus it is derived from Article 6.1 of the eIDAS Regulation, when it states that "when an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online", provided that it meets the requirements and conditions laid down in the Regulation and the corresponding implementing acts, to which we will refer shortly.

This recognition does not occur immediately, but is deferred over time, and more specifically, within a maximum period of one year since the publication of a list of identification schemes by the European Commission. However, in no case will cross-border recognition be applied before September 2018.

On the other hand, Article 6.2 of the eIDAS Regulation also determines that electronic identification systems that do not meet these requirements and conditions may also be subject to recognition by other Member States, albeit in a completely voluntary manner.

This legal effect of cross-border recognition of electronic identification is guaranteed only in relations between individuals and public sector bodies, which, in accordance with Article 3 (7) of the eIDAS Regulation, are defined as "a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate"; in a clear example of the connection of this institution with the policies of the European Union regarding the use of electronic means in the field of Member States' Public Administration.

Finally, it should be pointed out that national law may establish substantive legal effects in relation to one or more electronic identification systems. These effects may well include the full equation of an electronic identification system with a written signature, and although it is certainly a possibility that might be not justified, since it would collide with the signature or qualified electronic seal, it cannot be discarded. To do this, it should be a system that makes use of means of identification that allows the authentication of the data source and the integrity of the data, in addition to entity authentication, as for example in the case of an instrument such as an electronic national identity card (such as the Belgian eID, German nPA o Spanish DNI-e).

And it will happen, however, that this legal effect of equivalence will not enjoy cross-border recognition, unlike what happens with the figure of the qualified electronic signature provided for in the eIDAS Regulation, so surely such type of identification mean shall also be subject to the rules of electronic signature or seal.

3.3 *The rules for cross-border recognition of electronic identification means*

As indicated above, in order for this juridical effect of cross-border recognition to take place with respect to electronic identification systems, three conditions must simultaneously concur, according to Article 6.1 of the eIDAS Regulation:

- Firstly, the electronic identification means must have been issued under an electronic identification scheme included in a list published by the Commission, in accordance with Article 9 of the eIDAS Regulation itself, for which purpose there must have been notified in advance by the Member State.

- Secondly, the security level of this electronic identification means must correspond to a level of security equal to or higher than the level of security required by the public-sector body to access that online service in the first Member State, provided that the security level of the said electronic identification means corresponds to a substantial or high level of security.

- Thirdly, the public body in question must use a substantial or high level of security in relation to access to that online service, a provision which surprisingly precludes the possibility that a person with a better system than the requested by the public-sector body can actually use it, as for example will happen with a Spanish citizen who intends to use his electronic DNI to access a service in another Member State that only requires a low quality password, due to the low security sensitivity of the service.

3.3.1.1 Electronic identification systems that may be subject to notification

First, Article 7 (a) of the eIDAS Regulation states that the means of electronic identification under the electronic identification system must have been issued, alternatively, by the notifying Member State, at the request of the Member State making the notification, or independently of the Member State making the notification and recognized by that Member State.

This is a sample of the public service nature of electronic administration that permeates the regulation of electronic identification in the eIDAS Regulation, and represents a new sample of potential diversity among the Member States of the European Union. The eIDAS Regulation provides for up to three possible legal regimes for electronic means of identification, subject to notification, which have in common the necessary prior intervention of the State concerned for its cross-border recognition.

The first possibility is to notify an electronic means of identification issued by the Member State itself; that is to say, of their ownership, as for example would happen with systems such as the electronic DNI, the system Cl@ve PIN, MobileID, etc. The second possibility concerns the notification of an electronic means of identification issued by an entity other than the notifying State, but under its mandate, in accordance with national law.

These two first cases of issuing electronic identification means would be assimilated to true public services, at least in its broader or imprecise notion, which identifies it with general administrative activity. From this perspective, the main difference between the two cases would be given by the management modality of public service, which would be direct in the first case and indirect in the second case, being applicable the legal procedures established for the management of public services, depending on the type of Administration that is the owner or principal of the service, as well as the corresponding rules for public procurement.

However, depending on the case, we can also defend the issuance of electronic identification means as a public service in the strict sense, by concurring with the conditions that the doctrine has been demanding for it, as evidenced in cases such as the Spanish DNI-e or the German nPA, the issuance of which are reserved to the State. This consideration, referring to the identification means, is compatible with the broad notion of electronic public service on the globally considered identification system, which allows the coexistence of these monopolistic means with other private means.

Finally, the third possibility is based on the legal act of prior recognition by the State of an electronic identification system different from the previous ones – that is to say, issued independently of the State –, a category where we can include electronic identification systems operated by private entities, including financial entities, operators of electronic communications services, or providers of information society services, such as service portals Internet, or social networking, among many others. This would be the case of ARIES derived identities issued by the ARIES identity management service provider.

This third case is more complex, because the State is not the owner of the public service, nor is it provided under its mandate, in a scenario where the State could simply be just a consumer of the electronic identification means issued by private companies. Let us imagine, for example, that a State decides to acquire the right to use the electronic identification means supplied to citizens by a private entity so that they can access public services, instead of directly issuing them. It would not be appropriate if these means could not also be used for access to the public services of third-country bodies. Thus, this third case departs from the concept of public service and operates as a mechanism for extending the service acquired by State to the private sector, vis-à-vis third States. This is somewhat the case of countries as UK and, as you can guess, it is in this third possibility that we can find the most innovative and surely appropriate solutions to the nature of the Internet network, strongly marked by the intervention of multiple intermediaries, and, therefore, a new element of strong diversity among Member States of the Union.

This act of recognition of privately issued electronic identification means – that extends is usage to other Member States – is subject to national law and is not without major legal challenges.

Firstly, to the extent that the act of recognition has the legal effect of enabling the electronic identification means for use in cross-border authentication, the way in which it is exercised will have clear effects on the market. One possibility would be for the State to recognize all private providers who meet the conditions for this, although we could also find quantitative limits on the electronic identification means issued by private providers, forming a kind of virtual electronic public service.

In this case, the effects on free competition arising from, for example, recognizing a single private provider (or a small group of providers) should be carefully considered, since it could have a distorting effect on competition, granting these providers a competitive advantage that would foster the use of the same system in private transactions, probably under a fee.

Given that, as we have seen, electronic identification systems can be used perfectly for the accreditation of identity in electronic business processes – and, depending on the technology on which it is based, also for integrity and data origin authentication – they are functionally equivalent to electronic signature or electronic seal based in trust services, we must assume that the possibility of their use by private parties – for a price – can act as a limiting factor to the development of the trust services market. We therefore consider that the Member State which avails itself of this option must be diligent in selecting the identity providers it recognizes, guaranteeing reasonable conditions in relation to this activity.

And secondly, we must ask ourselves about the selection of the electronic identification system to be used, which we believe should be fully governed by national law and, more specifically, assuming that the provision of the service is not free for the Administration, by the rules of public procurement, currently contained Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (and the national implementations, of course), adopting the procedure that is most appropriate depending on the organization of the service. Although it is certainly not possible to rule out the possibility that the private provider of the electronic identification system does not charge any amount to the State that uses it, this possibility seems rather remote, given the obvious costs that this use may entail. Therefore, we would be faced with a potential service contract, if the Administration acquires the electronic identification system for itself (and possibly for private third parties), although it will also be possible to consider the possibility of an innovation partnership agreement.

Therefore, and in summary, it is appropriate to retain the fact that, overall, the electronic identification system is, in any case, configured as a public service, regardless of the consideration also as a public service, virtual public service or private service, of the issuance of electronic identification means within that same system.

3.3.1.2 The use of electronic identification for access to electronic public services in the issuing Member State

Article 7 (b) of the eIDAS Regulation requires that "the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public-sector body and which requires electronic identification in the notifying Member State". It is a requirement that connects, as we have previously seen, the instrumental nature of electronic identification with respect to access to public services, and its main legal consequence is to prevent the notification of systems that are not used for this purpose.

This provision can be understood as reasonable since, as we have seen, notification of an electronic identification system has the effect of imposing an obligation on the other Member States of the European Union to allow the use of such a system for cross-border access to their own systems of electronic administration. It would logically prove absurd that an electronic identification system issued in one Member

State which cannot be used in that Member State for access to eGovernment services could instead be used in the other Member States (especially in terms of liability).

This requirement may be an issue for the recognition of an ARIES derived identity, because it means that at least one EU government should previously accept the derived identity for an electronic government service.

3.3.1.3 The alignment of the scheme and the electronic identification means with a predetermined level of security

Article 7 (c) of the EIDAS Regulation requires that "the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8 (3)" of the regulation itself, so that those who do not meet those requirements would be excluded from this possibility of mutual recognition.

The difference between the system and the identification means brings into account the type of security measures to be considered, some of which fall under the management of the system, with a more intense approach to procedures, and others in the electronic identification means, with greater focus and detail in the corresponding technologies.

In any case, it must be remembered at this point that the recognition obligation only affects the electronic identification systems of substantial or high level, whereas, in the case of low level systems, such recognition is optional and, therefore, it will depend on the agreements to which the Member States may come with other Member States.

Security levels are described in Article 8.2 of Regulation eIDAS, as a number of - high-level and somewhat abstract - criteria that support a particular degree of confidence in the electronic identification means issued to the person, while reducing or avoiding the risk of misuse or undue alteration of identity.

Notwithstanding the analysis of the elements referred to each of the levels of security, it is necessary to remember that these levels differ according to the risk of use of the electronic identification in a specific service; that is, depending on the probability of occurrence of a threat, with a qualitatively or quantitatively determinable harmful impact, and that usually correspond to what in the standards is called "levels of authentication assurance".

The levels of security must be specified later, as provided in section 3 of Article 8 itself, in the following terms: "by 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1".

In this way, the European legislator seeks the cooperation of the EU Commission for the practical implementation of the aforementioned levels of security, using the indirect referral technique, and which is substantiated by an implementing act thunder the examination procedure. However, the European legislator lays down essential content for these minimum technical specifications, standards and procedures, which, according to the second paragraph of Article 8.3 of the eIDAS Regulation "shall be set out by reference to the reliability and quality of the following elements:

(a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) the procedure for the issuance of the requested electronic identification means;

(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;

(d) the entity issuing the electronic identification means;

(e) any other body involved in the application for the issuance of the electronic identification means; and

(f) the technical and security specifications of the issued electronic identification means".

This implementing act is Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) Nº 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS Security Regulation).

According to Recital (2) of the eIDAS Security Regulation, "determining the minimum technical specifications, standards and procedures is essential in order to ensure common understanding of the details of the assurance levels and to ensure interoperability when mapping the national assurance levels of notified electronic identification schemes against the assurance levels under Article 8 as provided by Article 12(4)(b) of Regulation (EU) Nº 910/2014". Thus, its purpose is twofold: on the one hand, to detail the criteria for the levels of security to obtain a common understanding of them; on the other, to facilitate the mapping between the levels of the Member State systems with the levels defined in the eIDAS Regulation.

It is interesting to note, firstly, that the eIDAS Security Regulation considers what is established in the international standard ISO/IEC 29115:2013, although it does not refer to any specific content of the same, because it "differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account", in accordance with its Recital (3). In addition, the eIDAS Security Regulation also considers the results of the STORK project, as mentioned in its Recital (4).

Secondly, according to Article 1(2) of the eIDAS Security Regulation, "the specifications and procedures set out in the Annex shall be used to specify the assurance level of the electronic identification means issued under a notified electronic identification scheme by determining the reliability and quality of following elements:

(a) enrolment, as set out in section 2.1 of the Annex to this Regulation pursuant to Article 8(3)(a) of Regulation (EU) Nº 910/2014;

(b) electronic identification means management, as set out in section 2.2 of the Annex to this Regulation pursuant to Article 8(3)(b) and (f) of Regulation (EU) Nº 910/2014;

(c) authentication, as set out in section 2.3 of the Annex to this Regulation pursuant to Article 8(3)(c) of Regulation (EU) Nº 910/2014;

(d) management and organisation, as set out in section 2.4 of the Annex to this Regulation pursuant to Article 8(3)(d) and (e) of Regulation (EU) Nº 910/2014".

The notion is that the Regulation we are examining will determine, for each of these elements, one or more specifications and/or procedures, which will help Member States to rely on the electronic identification means.

First, section 2.1 of the Annex to the eIDAS Security Regulation refers to the registration in the electronic identification system, in relation to which it determines criteria for the application and registration; The proof and verification of the identity (of natural person, of juridical person); And the link between the means of electronic identification of physical and legal persons. This section contains the appropriate controls for the registration of a new user in an electronic identification system, often also called "registration phase", as in the STORK QAA framework.

Secondly, section 2.2 of the Annex to the eIDAS Security Regulation refers to the management of electronic identification means, establishing criteria referring to the characteristics and design of electronic identification means; to the expedition, delivery and activation thereof; suspension, revocation and reactivation thereof; and to the renewal and replacement of these same means. In this case, an approach to management processes organized around the life cycle of the means of electronic identification, or credentials, is adopted, which will require corresponding adaptations to each technology.

Thirdly, section 2.3 of the Annex to the eIDAS Security Regulation refers to authentication, in relation to which essentially establishes requirements related to the authentication mechanism, through which the natural or legal person uses the means of electronic identification for Confirm its identity to the user side. That is, in this phase is where the person uses his credential to claim his identity to the service he intends to access, using the corresponding technical protocol, so it should be noted that this process only allows to rely on the identification data of the person, and does not assert anything about the suitability of such data for the purposes of the service to which the person us granted access.

Finally, section 2.4 of the Annex to the eIDAS Security Regulation concerns the management and organization of participants providing a service related to electronic identification in a cross-border context, including certain general provisions; publication of notices and user information; information security management; conservation of information; facilities and staff; technical controls; and compliance and audits.

The implications of this requirement for the ARIES project are really critical, because if the ARIES service is not aligned with at least the substantial security level, it will be more than difficult to gain general recognition for it, at least under the eIDAS Regulation.

3.3.1.4 The exclusive attribution of the electronic identification data and means

As a specification of the alignment requirement with a predetermined level of security, Article 7 (d) and (e) of the eIDAS Regulation require the guarantee of exclusive attribution of electronic identification data and means to the person concerned.

In the first case, it is required that “the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued”.

We can recall the identification data are those that allow the identification of the person, such as in the case of an electronic certificate, or an identity card contained in a database.

This guarantee must be offered in the terms of the implementing act that defines the levels of security, which we will present later, and must be offered at the moment in which the means of identification are issued; it is a requirement of what is known as the user "registration", and it is very significant that this

obligation is imposed on the State – and with the corresponding liability – and not on the entity that issues the electronic identification means, something that accounts for the fundamental importance of digital identity.

In the second case, though, it is required that "the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8 (3)" of eIDAS Regulation.

In this case, it is the party that issues the electronic identification means who must offer this guarantee – and assume the corresponding liability – something that is understandable given that it is the entity that takes charge of the operation of the system, having to do it with the minimum mandatory security measure we will present later.

The identification data are defined in the Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12 (8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Interoperability Regulation).

In this sense, Article 11 of the eIDAS Interoperability Regulation authorizes the use of various attributes for the representation, in an electronic identification means used in a cross-border context, of the identity of a natural or legal person (section 1), or of a natural person who represents a legal person (section 2), specifying that "data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters" (section 3).

The purpose of this rule is to agree on the minimum mandatory contents to be used for the description of a natural or legal person, in a cross-border context. Given that the different identity numbers or codes assigned by the authorities of the Member States – which will be employed by the identity providers of those Member States – may be incomprehensible to service providers in other Member States, or that there may be legal issues for the cross-border use of an identity code, as they are of exclusive use within the Member State, it is necessary to establish rules for the assignment of specific identifiers for cross-border authentication, or for the use of previous identifiers for cross-border transactions. I.e., in Germany it is not allowed to use the national identification number outside Germany, and thus it is necessary to assign a new identifier, which will be valid for that specific type of transaction (a kind of derived identity).

In this sense, section 1 of the annex to the eIDAS Interoperability Regulation imposes the obligation to use the following attributes for the identification of a natural person: a) surname or current surnames; b) current name or names; c) the date of birth and d) a unique identifier drawn up by the issuing Member State in accordance with the technical specifications for cross-border identification purposes and as constant as possible over time.

Likewise, the following additional attributes are authorized: a) name or names and surname or surname of birth; b) place of birth; c) current address and d) sex; being understood that whenever the necessary prior consent is available, except in those cases where the legislation excludes it.

Technical specifications have been established in the STORK projects, for cross-border identification, based on a set of principles that seek to reconcile the different legal sensitivities of Member States with regard to the use of identifiers. That means that the ARIES protocols should be aligned with these technical specifications, at least to be interoperable in the EU context.

3.3.1.5 The availability of an online authentication mechanism

Article 7 (f) of the eIDAS Regulation requires that "the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form", when the said person needs access to a service offered online by that party.

In our opinion, this obligation is essential for the operation of the electronic identification system, since the relying against which the person is to be identified needs to be able to verify that the person is who she claims to be, according to the technological system used, and therefore is imposed on the corresponding identity provider, to which the State must transfer this legal obligation.

However, the obligation under this heading should also be understood as referring to the need for the State to establish and guarantee the overall operation of the electronic identification system, as well as one or more nodes of the interoperability architecture for electronic identification, all subject to an electronic public service regime reserved to the competent public authority in each Member State. Again, this is an electronic public service, with a marked instrumental nature, facilitating the provision of other finalist public services or the performance of electronic administrative procedures, especially from the perspective of relationship with the citizen; but also in support of the realization of private sector transaction, and thus it can eventually overcome the wards of so-called e-Government, affecting market development.

The relying party must access this process of cross-border authentication online, so that, if it is not available, access to the service offered by the relying party is simply interrupted. Consequently, it is configured as a mandatory service and, as we have seen, is regulated by public law, regardless of the ownership of the electronic identification device issued – and the corresponding authentication process –, or also the ownership of the service which is accessed through the aforementioned authentication.

According to the second paragraph of this paragraph (f), "the cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body", a requirement which is aptly intended to avoid the complex and problematic Invoicing for the consumption of the service between the different Member States of the European Union, and from which we can also infer to the contrary that a fee for the use of this service may be established in other cases – as in the same paragraph is to be understood when it states that "for relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication".

That the process of cross-border authentication is free when used for access to electronic public services implies, on the other hand, that the use of the electronic identification means for such authentication must also be free; that is to say, both the use of the electronic identification means (such as the electronic National ID, or a qualified certificate, or a password) and the technical platform implementing the authentication process must be free of charge, regardless of the ownership of the electronic identification means. Thus, in case the identification means is offered by a private company, free usage will be a condition required for recognition. This condition may make commercially uninteresting for private providers offering the service to its customers, at least for the cross-border authentication when accessing public services.

Finally, the second paragraph of this numeral requires that "Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes", in order to maximize the potential use of electronic identification means in cross-border online authentication.

This provision refers to the relying parties in the system, which will be, mainly, public sector bodies of the Member States other than the one in whose territory the electronic identification means has been issued, but in the end, it protects the citizens having the aforementioned means, who are interested in being able to authenticate themselves to e-government or other services on the territory of another Member State.

What is to be considered as a disproportionate technical requirement, and under what circumstances does it impede or significantly impede interoperability, is a factual issue to be resolved on a case-by-case basis, but imposition of software installation or use by the citizens are a good candidate. We are referring to additional technical conditions different from those which form part of the framework of interoperability provided for in the Regulation itself, even if formally compatible with it.

It is true that the very existence of the eIDAS interoperability framework, and its subsequent application by the Member States, can provide elements that help to objectify these circumstances, reinforcing their relevance as a public soft law instrument.

3.3.1.6 Prior cooperation

Article 7 (g) of the eIDAS Regulation requires the Member State aiming to notify the European Commission of an electronic identification system that, at least six months prior to such notification, notify the other Member States a description of the system in advance.

The purpose of this action is to inform the other Member States of the European Union about the system envisaged to be notified, for the purposes of cooperation between them, as provided for in the Regulation, which is aimed at the interoperability and security of the identification system subject to notification.

The eIDAS Regulation does not define precisely the content of this description of the system, but we can understand that it will be the same description provided for in Article 9.1.a) of the same, as part of the contents of the notification to be sent to the European Commission.

This is clear from Article 13 of Commission Implementing Decision (EU) 2015/296 of 24 February 2015, which obliges the Member State to refer to the Cooperation Network the draft notification form with the contents provided for in Article 9.1.a) of the eIDAS Regulation.

3.3.1.7 The guarantee of interoperability of electronic identification means

Finally, Article 7 (h) of the eIDAS Regulation requires that, in order to be notified, an electronic identification system must comply with the provisions of the interoperability framework provided for in Article 12.8 of that Regulation, approved by the aforementioned eIDAS interoperability Regulation.

4 Use of advanced electronic signatures based on qualified certificates issued by an ARIES provider

One possible implementation of the ARIES service implies the usage of advanced electronic signatures based on qualified certificates that are issued by the ARIES provider - or by a third party acting on behalf of the ARIES provider – to the ARIES user, a legal institution that is currently regulated in the eIDAS Regulation.

Moreover, the issuance of qualified certificates is considered, in the eIDAS Regulation, as a qualified trust service in support of advanced electronic signatures, or other uses, including identification. This is due to the fact that an advanced electronic signature "is capable of identifying the signatory", according to Article 26 (b) of eIDAS Regulation, especially when it is based on a qualified certificate, because a certificate "means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person" (Article 3 (14) of eIDAS Regulation) and this confirmation is presumed to be legally true when the certificate is qualified.

Therefore, and ARIES provider may implement its services by issuing qualified certificates, and for that, it must become a qualified trust service provider. We need, then, to review what a trust services is, and what is the legal regime under this "qualification".

According to Article 3 (16) of the eIDAS Regulation, 'trust service' means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
(b) the creation, verification and validation of certificates for website authentication; or
(c) the preservation of electronic signatures, seals or certificates related to those services;"

This Article does not properly contain a definition or concept of trust service, but rather an enumeration of information society services which, precisely because they are included in the closed list, are considered to be "trustworthy".

This notion of "trust service", also referred to as "reliable service" or "trusted service", is not an invention of the eIDAS Regulation, but rather has been used for a long time by market agents, as well as by scholars. For example, Olnes[1] defines trust as the perception of absence of vulnerabilities and, after distinguishing between technical and organizational trust, offers a taxonomy of reliable services attending to some characteristics of such services, such as type of service, quality of service, evidence management, user community, trust model, legal aspects and communications pattern.

Baldwin, Shiu, & Cassasa Mont[2] refer to trusted services as e-commerce enablers and indicate the existence of trusted services widely installed in paper processes, considering that service providers are experts managing risks related to the services they offer, and provide a list of services candidates to enter this qualification: identity, authorization, anonymity, qualification and trust recommendation, guarantee of

[1] Olnes, J. (2001). A Taxonomy for Trusted Services. In B. Schmid, K. Stanoevska Slabeva, & V. Tschammer (Eds.), Towards the E-Society: E-Commerce, E-Business, and E-Government (Vol. 74, pp. 31-44). Kluwer Academic Publishers.

[2] Baldwin, A., Shiu, S., & Cassasa Mont, M. (2002). Trust Services: A framework for service-based solutions. Proceedings of the 26 th Annual International Computer Software and Applications Conference (COMPSAC'02) (pp. 507 -513). IEEE.

delivery of communications, generation of auditable receipts, storage and notarization. These authors also refer to the existence of certain services of trustworthy components, which are meaningless to end users, but which are used in other trusted services, including key storage services, archiving services and date and time stamp services.

For Dumortier & Vandezande[3], trust in e-commerce operations works in a similar way to a black box: the user is confident that the machine will record all processes and maintain sufficient evidence to be able to reproduce what really happened; an approximation they consider that may be more effective than the use of electronically signed documents. In their opinion, and regardless of the definition or concept of trust, it always consists of an internal state of the user evoked by the reliability characteristics of the technology, being an informed acceptance of the vulnerability.

In short, we could conceptualize trusted services as those technologies that can be trusted, modifying the user's perception regarding the vulnerability of a process to which they are incorporated. For this, the user must be able to recognize a trust service, in fact, as secure and reliable enough. To do this, the approach of the eIDAS Regulation is the creation of a reinforced level of services of trust, which is significant in the sense that the trust in these services seems to be born from the fact that they are legally regulated, rather than only in their own technical characteristics.

In this sense, Article 3 (17) of eIDAS Regulation provides the notion of a "qualified trust service", defining it as "a trust service that meets the applicable requirements laid down in this Regulation", which differentiates two "reliance levels":

- The non-qualified level of a trust service, which is not practically regulated, and does not receive any particular legal recognition; and in which case, the user must construct his own internal state of trust with respect to the service. For example, a person can recognize a password from your financial institution as being secure enough, but not a cloud storage service.

- The qualified level of trust service, which is highly regulated, and receives a particular recognition of legal effects, something which should be an incentive to its adoption. In this case, this explicit legal recognition is the one that allows the user to recognize the service as reliable, so we can assume that these services will be developed earlier and in greater volume than those that do not enjoy this condition.

It should also be noted that the eIDAS Regulation contains a closed list of trusted services in order to delimit the scope of the uniform European regulation but that Member States may define other trust services as well as maintain (or introduce) national provisions, in accordance with Union law, concerning trust services of confidence, provided that such services are not fully harmonized by this Regulation, considerations which show the central objective of the regulation, which is none other than to guarantee the free movement of these services in the internal market, by means of a minimum set of harmonized standards.

One consequence of this model is the more than possible divergence in the catalogue of trust services in the different jurisdictions of the European Union, as the business sector is constantly generating new services, based on technological innovation. One good example is precisely the ARIES project.

[3] Dumortier, J., & Vandezande, N. (2012, October). Trust in the proposed EU regulation on trust services? Computer Law & Security Review, 28(5), 568-576. doi:10.1016/j.clsr.2012.07.010

As we have pointed out, and in contrast to the Electronic Signature Directive, where the provision of certification services was completely free, the eIDAS Regulation opts for a regulatory orientation of prior administrative authorization in relation to the provision of qualified trust services, while maintaining the *ex post* supervision model for non-qualified services.

Indeed, Article 21 (1) of the eIDAS Regulation sets out that a provider, who does not have a qualification, to begin its activity relating to qualified services, must submit to the supervisory body a notification of his intention together with a conformity assessment report issued by a conformity assessment body, whereas Article 17 (3) (a) (4) (g) stipulates that the national body will carry out prior supervision and the award of the qualification, and that the service cannot be started until such qualification has been obtained (Article 21.3), and it has been publicly disseminated through the mechanism provided for in Article 22 of the eIDAS Regulation (the Trust Service List). Although with a somewhat obscure terminology, this is an administrative authorization, which must be granted under the relevant administrative procedure, within the framework of national legislation.

In addition, the qualified provider of trusted services must pass a conformity assessment at least every two years and send it to the supervisor, as determined by Article 20.1 of the Regulation, as well as accept any audit performed by the supervisor, or additional assessments of conformity that it imposes on it, pursuant to the provisions of paragraph 2 of Article 20 of the eIDAS Regulation.

It is also interesting to note that qualified trust services have a strict liability regime contained in Article 13 (1) of the eIDAS Regulation. In its virtue, "trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation" (subparagraph 1), and "the intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider" (subparagraph 3); while in the case of non-qualified trust services, "the burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph" (subparagraph 2).

This new regulatory approach is a clear exception to the approach of the e-Commerce Directive, which in its Article 4 prohibits the subjection of information society services to prior authorization or any other requirement with equivalent effect, and Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, which limits the possibility of restricting access to and Authorization only in certain circumstances.

That doesn't mean that the rest of the regulation of the information society services does not apply. On the contrary, any provision in that regulation that doesn't conflict with the trust services regulation will be applicable to the ARIES service.

The legal regime of qualified trust services included in the eIDAS Regulation has been partially developed by the following implementing acts:

- Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance).

  This implementing act is relevant for the ARIES project because it allows the ARIES provider to easily prove that it is issuing qualified certificates, facilitating the adoption of the derived identities by relying parties. According to Article 23 (1) of the eIDAS Regulation, "after the qualified status

referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide".

- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

  This implementing act is also relevant for the ARIES project because these formats have the legal admissibility granted in relationships with public sector bodies.

- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

An ARIES provider may play two different roles under the concept of trust services:

- ARIES provider may issue qualified certificates assuring the identity of the person, using pseudonym certificates and other attributes, as a means to represent derived identities. This possibility is directly implementable in the current EU framework, but its recognition is subject to the authorisation of the usage of pseudonym certificates in each Member State.

- ARIES provider could offer a new trust service, consisting on the accreditation of possession of personal attributes (a wide conceptualization of identity) with privacy protection. This may be considered as the main legal innovation of the project: an ARIES provider, once a person identity has been provisioned, provides a service that allow 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 constitute assertions that may legally substitute 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.

  To be able to substitute these documents per partial derived ARIES identities, maintaining legal certainty, we shall propose the definition of this services a new trust service, defining the service and a legal effect attained to the service (i.e. establishing some sort of equivalence principle such as "where the law requires the documental accreditation of a personal attribute, it will be possible to use a [service name] evidence".

  Thus, the implementation of this possibility, which will be further analysed during the rest of the project, it will be needed to adopt it as a new trust service, ideally at the EU level, or at the Member State level (a more realistic scenario).

5 Personal data and law enforcement aspects

5.1 *Legal requirements related to personal data general regulation*

The ARIES project involves the processing of personal data wholly or partly by automated means and therefore the GDPR has to be applied. Although its provisions will not completely be into force until 2018, the end of ARIES project beyond that date determines that any legal analysis necessarily has to consider them. The GDPR has only set up a minimum set of rules in order to adapt the legal guarantees of data flows among EU. It is "intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons" (Recital 2).

Within this context, the current Directive 95/46/EC has not fulfilled one of its main goals: to achieve a certain degree of harmonization and, therefore, it has not prevented fragmentation in the implementation of data protection across the Union. That is the reason why the GDPR tries to set up a level of protection of the rights and freedoms of natural persons with regard to the processing of their data that should be equivalent in all Member States. Nevertheless, its provisions may be completed by Member States as they are allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation.

Member States are in the way of adopting their own national rules that are expected to by finally passed before 25 May 2018, when the GDPR will apply. This delay implies an additional difficulty for studying the concrete legal requirements for the project in this field since the ARIES provider will be also subjected to the national data protection framework where it has been established. In order to tackle this challenge an intermediate PIA will be prepared during the first term of 2018, which will be used as the legal background for D.2.4 (*Privacy and data protection compliance report*) scheduled for M24. It will also be a useful tool to take into account further legal requirements since the EU legal framework is still incomplete from the perspective of ARIES project, since a very relevant piece is still being prepared. On 10 January 2017 the Commission has presented a proposal for a *Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC) (ePrivacy Regulation)*. Although the relationship of this future Regulation with the GDPR is not clear and completely defined[4], once it is finally approved a new assessment of the legal requirements has to be made in order to assure that the ARIES project complies with all the legal requirements related to data protection issues.

Anyway, it was completely necessary for the aim of this report to study the implication of the general data protection framework from the perspective of the ARIES legal requirements. In fact, as we will insist below, the GDPR not only has established the legal conditions for processing the users' data but for legal enforcement as well, particularly from the perspective of access by the competent authorities in those cases not related to criminal offences.

First of all, from the position of the user, the ARIES provider is obliged to obtain its consent as a consumer as it was previously stated. From this voluntary basis, although a specific consent for data process is not generally required by the GDPR, signing up for ARIES services hast to include necessarily this requirement as part of a contractual relationship.

[4] European Data Protection Supervisor: *Opinion 5/2016. Preliminary Opinion on the Review of the ePrivacy Directive*, page 9.

Nevertheless, ARIES involves processing of biometric data and, although it is not allowed as a rule according to Article 9 GDPR, this interdiction does not apply if the data subject has given explicit consent to their processing for one or more specified purposes. Therefore, the ARIES provider has to record users' consent in a proper way in order to answer a data owner's claim or to face an inspection from a supervisory authority. A way for withdrawing their consent has to be offered to the users as well when they decide to give up ARIES services and the date of this action has to be registered. Nevertheless, the withdrawal will not affect the obligation of the ARIES provider to store those data that may be relevant in the event of a claim or a law enforcement demand of information made by the judicial o police authority. The withdrawal procedure has to be as easier as giving the consent but it will not imply deleting all the data concerning the users since ARIES has to store them during the period fixed by the Member State's law where it is stablished.

The general terms and conditions that have to be accepted by users when signing up ARIES services should contain a data protection clause including all the requirements of Article 13 GDPR:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
b) the identity of the potential recipients to whom the personal data will be disclosed, including law enforcement agencies;
c) the contact details of the data protection officer;
d) the recipients or categories of recipients of the personal data;
e) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
f) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
g) the right to lodge a complaint with a supervisory authority;
h) that the provision of personal data is a requirement necessary to enter into a contract;
i) that the data subject is obliged to provide the required personal data to gain access to ARIES services;
j) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.

Regarding this last requirement, Article 13.3 GDPR states that when "the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information". Apart from any other purpose, there is a clear obligation for the ARIES provider in order to transfer information about the users to law enforcement authorities and, consequently, it should inform the users about this eventual data process. The concrete conditions and limitations under which those authorities can access to ARIES users' data will be analyzed in the following section of this report.

In the event of further commercial and/or commercial purpose of the ARIES users' data, apart from the obligations related to information, the importance of respecting the purpose limitation principle has to be underlined. As one of the main guarantees of personal data protection as a fundamental right across, the UE. Article 5.1.b) GDPR bans to use them in a manner that is incompatible with those initial purposes; and it also act as a limit for the storage of the data linked to a concrete user during the period required by those purposes. Therefore, the ARIES provider shall make an inventory of all the specific purposes for which personal data are going to be processed in order to determine the scope of that limitation for further uses.

Regarding the notion o*f incompatibility*, the UE legislator imposes a double negation: personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. As the Article 29 Working Group has stated, "the fact that the further processing is for a *different* purpose does not necessarily mean that it is automatically *incompatible*: this needs to be assessed on a case-by-case basis"[5]. Apart from those cases where the answer to the compatibility test is obvious and does not need a deeper analysis, the assessment has to include several criteria that may help the data controller to motivate its decision; particularly the relationship between the new and the old purpose and the context where data were collected[6]. For the ARIES case, data will be collected from users when they sign up its services in order to provide them with identification tools in a context of privacy protection scheme. Therefore, as trust is one of the most relevant values in the ARIES ecosystem, the use of the users' data may not be considered compatible for any other commercial purposes. Anyway, for the airport scenario, the use of Passenger Name Record (PNR) must be strictly restricted to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes. Consequently, any different use would not be justified according to Directive (EU) 2016/681.

This legitimate purpose —providing both the users and third parties with identification services— also implies a limitation of the maximum period of storage of the data linked to a concrete user. As Article 5.1.e) GDPR states, they "may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest". Law enforcement may demand a longer period of storage, but the specification of this requirement remains as a competence of Member States and, therefore, this relevant question cannot be answered generally. Anyway, Article 89 GDPR requires that processing for archiving purposes in the public interest has to be subject to appropriate safeguards according to the principle of data minimisation, that may include pseudonymisation as this purpose can be fulfilled in that manner. Nevertheless, there must be a way to re-identify the user in order to make the information available to a competent public authority.

As a data controller, the ARIES provider shall also create a record of processing activities. This record has to adopt the adequate security measures for storing and processing users´ personal data taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. From the perspective of privacy by design requirements, access must be limited only to those data necessary to provide the services (minimisation). Due to its importance for the project, these technical and organisational measures have been determined in a specific document, which is the *Data Minimization and Privacy by Design Guidelines* (MS5) that was made available to all partners in M8.

From the perspective of users, a concise, transparent, intelligible and easily accessible form, using clear and plain language, shall be offered by the AIRES provider in order to enable them to exercise their rights to access, to rectification inaccurate data concerning them, to erasure their data when a legal provision applies, to restriction of processing them (with the exception of storage). Finally, the ARIES provider has to be able as well to allow users' access to their own data in a structured, commonly used and machine-readable format.

5.2 *Access of law enforcement authorities to the ARIES provider information about the users*

Law enforcement agencies has to be also considered as end-user in the ARIES project as one of its main goals is to address the new threats in pursuing identity theft related to cybercrime. Therefore, a special attention has to be paid to the conditions of their access to the information existing in the ARIES Secure Vault in order

[5] Article 29 Data Protection Working Party: *Opinion 03/2013 on purpose limitation*, 00569/13/EN WP 203, page 21.

[6] Article 29 Data Protection Working Party: *Opinion 03/2013 on purpose limitation*, 00569/13/EN WP 203, page 22.

to check the transaction logs stored in the vault in case of identity fraud, misuse, liability or cybercrime investigation.

GDPR rules do not cover how personal data can be used for law enforcement purposes in those areas. These issues fall under the separate legal instrument known as the Law Enforcement Directive. According to the scope of this Directive, it "lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". Its provisions are strictly limited to the police and criminal justice authorities since they are justified on the specific nature of these sectors as Article 16 of the *Treaty on the Functioning of the European Union* states[7]. Consequently, as a private body, they may only be applied to the AIRES provider indirectly since the main legal conditions and limits of its activity from the perspective of personal data are those required by the GDPR provisions.

The Law Enforcement Directive entered into force on 5 May 2016, but Member states have until 6 May 2018 to translate its provisions into their national legal frameworks. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject. The lack of a harmonized legal framework for gain access to those data in this field implies that every Member State may impose different conditions to law enforcement agencies. However, once the information is obtained, some general legal requirements should be taken into account when processing those data, particularly from the perspective of the Law Enforcement Directive.

The ARIES provider should only give access to the Secure Vault according to the legal framework of the Member State where it is established. Each Member State is allowed to specify the objectives of processing, the personal data to be processed and the purposes of the processing. Consequently, the particular conditions to which the ARIES users' data will be subjected for the above-referred purposes —criminal offences and penalties, as well as public security issues— cannot be fixed at this stage, and therefore this report will only focus on the general ones stablished at the EU level. Anyway, it must be highlighted that, as Article 3.10 of the Law Enforcement Directive states, any "public authorities which may receive personal data in the framework of a particular inquiry in accordance with Member State law shall not be regarded as recipients".

Apart from the controversial relationship between the general provisions of GDPR and de Law Enforcement Directive[8], the purpose for which law enforcement authorities demand access to users' data is certainly essential for the legal framework to be applied. If the data are to be used out of the scope of the Law Enforcement Directive, then the GDPR requirements will be applied as Article 9 stablishes. This would happen when the judicial inquiry is related to other fields or if an administrative body requires the information.

Anyway, regardless the legal framework that has to be applied, access to personal data by public authorities implies a restriction of this fundamental right and consequently its scope should be interpreted restrictively. This is an essential requirement since, as a general tendency, on one hand the EU has gradually widened the use of personal information for law enforcement purposes[9] and, on the other hand, there is now a tendency to require that private actors co-operate with law enforcement authorities on a systematic basis. According

[7] *Declaration (21) on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the Lisbon Treaty*.

[8] European Data Protection Supervisor: *Opinion 6/2015. A further step towards comprehensive EU data protection EDPS recommendations on the Directive for data protection in the police and justice sectors*, page 4.

[9] Blasi Casagran, C. (2016). *Global Data Protection in the Field of Law Enforcement: an EU Perspective*. Routledge, p. 23.

to this condition, the ARIES interface shall implement secure communication, strong authentication and authorization mechanisms, and enable the law enforcement agency to retrieve requested information among the different transactions on READ-ONLY basis. All the requests will be logged to keep the full history of investigation events since, as Article 6 Law Enforcement Directive states, the AIRES provider might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings and is obliged to provide information on criminal offences. Finally, the ARIES interface should inform the law enforcement authority that the information obtained cannot be processed for purposes incompatible with those of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The need of a restrictive interpretation is not contrary to the interdiction of incompatible further uses: although users' data were originally collected and generated for the purpose of providing identity services for private users, it is clearly proportionate and justified to use them for law enforcement purposes as well [10]. Consequently, respecting the legal national and EU framework is an essential condition in order to assure that data processing is carried out in both fairly and legally conditions; making compatible the controversial conflict between data protection and public interest[11].

Therefore, although they should be informed about this possibility when signing up the ARIES services, the consent of ARIES users is not necessary and should not provide a legal ground for processing personal data by competent authorities. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require ARIES to comply with any request of information that respect the legal requirements.

Nevertheless, the European Court of Justice has clearly stated that access of public authorities on a generalised basis to the content of electronic communications affects the very essence of the right to privacy[12]. According to this vision, the ARIES provider cannot set up a general surveillance system for all users in order to give access to law enforcement authorities to all users' data, but it is obliged to reveal them in the context of a concrete inquiry. As Recital 21 of Law Enforcement Directive clearly demands, "the requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems".

Even more, the request has to be made by the competent authority in the Member State where the ARIES provider is stablished and this demand must respect the general legal conditions imposed by the national regulation. As the EU legal framework has not stablished a general obligation of providing the information regardless the nationality of the law enforcement authority, the general ways as of judicial and police cooperation should be used in this case[13]. The Europol's Secure Information Exchange Network Application (SIENA) should therefore be Member States' channel of first choice for law enforcement information sharing across the EU since it allows them to

[10] Blasi Casagran, C. (2016). *Global Data Protection in the Field of Law Enforcement: an EU Perspective*. Routledge, p. 26.

[11] *Communication from the Commission to the European Parliament and the Council. Stronger and Smarter Information Systems for Borders and Security* (COM(2016) 205 final), pp. 4-5.

[12] Judgement of the Court (Grand Chamber) 6 October 2015, case C-362/14 (Maximillian Schrems).

[13] Although effective and efficient cross-border collaboration is key, both within the EU and with third countries, bureaucracy and formalities involved in international cooperation means that is it not used as much as it could (Centre for Strategy & Evaluation Services: *Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft. Final report*, 2012, pages 105-106).

exchange information in a swift, secure and user-friendly way with each other, with Europol, or with third parties that have a cooperation agreement with Europol[14].

[14] Communication from the Commission to the European Parliament and the Council: *Stronger and Smarter Information Systems for Borders and Security* (COM (2016) 205 final), page 6.

6 Other legal requirements applicable to ARIES ecosystem participants

Legal requirements related to the application of consumer rights legislation

In some cases, the person receiving the ARIES service will be acting for purposes which are outside his trade, business, craft or profession, and therefore will be considered a consumer. In this case, the ARIES provider will be considered as a trader concluding a service contract with the consumer.

Generally, this service contract will be a distance contract; that is, a contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded.

Thus, any legal requirement related to consumers should be considered when implementing the ARIES services, as detailed in the Annex of this document.

Legal requirements related to the application of information society services legislation

The ARIES service may be considered, from a legal perspective, as an information society service, according to the definition contained in Article 1(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services; that is, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition, the Directive sets out the following definitions:

(i) 'at a distance' means that the service is provided without the parties being simultaneously present;
(ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
(iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

ARIES services should therefore comply with any relevant legal requirement set forth in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), as detailed in the Annex of this document.

Bibliography

Alamillo Domingo, I. (Junio de 2014). El nuevo Reglamento europeo de servicios de confianza digital: ¿fin de la libertad o principio de calidad? *Revista SIC*(110).

Atzeni, A., & Lioy, A. (2011). *STORK. D2.4 – Mapping of the national authentication levels of the new Member States to the STORK QAA levels.* STORK-eID Consortium. Obtenido de https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1876

Baldwin, A., Shiu, S., & Cassasa Mont, M. (2002). Trust Services: A framework for service-based solutions. *Proceedings of the 26 th Annual International Computer Software and Applications Conference (COMPSAC'02)* (pp. 507-513). IEEE.

Blasi Casagran, C. (2016). *Global Data Protection in the Field of Law Enforcement: an EU Perspective*. Routledge.

Borges, G. (2012, 09 05). The Draft Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM (2012) 238. *Presentation at the Workshop on Electronic Identification and Trust Services*. Brussels.

Brugger, J., & Fraefel, M. (2013). *STORK 2.0. D.7.3 Business Plans - Consolidated Report & Recommendations.* STORK 2.0 Consortium. Obtenido de https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=40:d731-business-plans-consolidated-report-a-recommendations&Itemid=177

Brugger, J., Fraefel, M., Meerbergen, P., Van der Donckt, C., Riedl, R., & Sánchez, J. (2014). *STORK 2.0. D.7.2 Service Design and Pricing - Consolidated Report & Open Questions.* STORK 2.0 Consortium. Obtenido de https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=39:d72-service-design-and-pricing-consolidated-report-a-open-questions&Itemid=177

Centre for Strategy & Evaluation Services (2012). *Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft. Final report*.

Clowes, N., & Brathwait, L. (2009). *STORK. D4.2 Final report on eID process flows.* STORK-eID Consortium. Obtenido de https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=952

Dumortier, J., & Vandezande, N. (2012, October). Trust in the proposed EU regulation on trust services? *Computer Law & Security Review, 28*(5), 568-576. doi:10.1016/j.clsr.2012.07.010

Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., & Van Eecke, P. (2003). *The legal and Market Aspects of Electronic Signatures: Legal and market aspects of the application of Directive 1999/93/EC and practical applications of efectronic signatures in the Member States, the EEA, the Candidate and the Accession countries.* Interdisciplinary centre for Law and Information Technology, Katholieke Universiteit Leuven. Obtenido de http://skilriki.is/media/skjol/electronic_sig_report.pdf

Eertink, H., Hulsebosch, B., & Lenzini, G. (2008). *STORK. D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme.* STORK-eID Consortium. Obtenido de https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=579

Graux, H., & Majava, J. (2007). *eID Interoperability for PEGS. Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms.* European Communities. Obtenido de http://ec.europa.eu/idabc/en/document/6484/5938/

Graux, H., & Majava, J. (2007). *eID Interoperability for PEGS. Summary of existing national and other authentication schemes.* European Communities. Obtenido de http://ec.europa.eu/idabc/en/document/6484/5938/

Graux, H., Majava, J., & Meyvis, E. (2009). *Study on eID Interoperability for PEGS: Update of Country Profiles. Analysis & assessment report.* Obtenido de http://ec.europa.eu/idabc/en/document/6484/5938/

Heppe, J. (2010). *STORK. D4.3 Updated Report on eID Process Flows.* STORK-eID Consortium. Obtenido de https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1875

Heppe, J., Berbecaru, D., Jorquera, E., Schiavo, M., Johnston, A., Lioy, A., . . . Bauer, W. (2011). *STORK. D5.7.3 Functional Design for PEPS, MW models and interoperability.* STORK-eID Consortium. Obtenido de https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1874

Hulsebosch, B., Lenzini, G., & Eertink, H. (2009). *STORK. D2.3 - Quality authenticator scheme.* STORK-eID Consortium. Obtenido de https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

ISO/IEC. (1996). *International Standard 10181-2. Information technology - Open systems interconnexion - Security frameworks for open systems: Authentication framework.*

ISO/IEC. (1996). *International Standard 10181-6. Information technology - Open systems interconnexion - Security frameworks for open systems: Integrity framework.*

ISO/IEC. (1997). *International Standard 10181-4. Information technology - Open systems interconnexion - Security frameworks for open systems: Non-repudiation framework.*

ISO/IEC. (1998). *International Standard 9798-3. Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques.*

ISO/IEC. (2009). *International Standard 9798-5. Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero-knowledge techniques.*

ISO/IEC. (2010). *International Standard 9798-1. Information technology - Security techniques - Entity authentication - Part 1: General.*

ISO/IEC. (2011). *International Standard 24760-1. Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts.*

ISO/IEC. (2013). *International Standard 29115. Information technology - Security techniques - Entity authentication assurance framework.*

ISO/IEC. (2015). *International Standard 2382. Information technology - Vocabulary.*

ISO/IEC. (2015). *International Standard 24760-2. Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements.*

ITU-T | ISO/IEC. (2012 | 2014). *Recommendation X.509 | International Standard 9594-8. Information technology - Open Systems Interconnection - The Directory - Public-key and attribute certificate frameworks.*

Khatchatourov, A., Laurent, M., & Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption. En E. Tambouris, M. Janssen, H. J. Scholl, M. A. Wimmer, K. Tarabanis, M. Gascó, . . . P. Parycek, *Electronic Government. 14th IFIP WG 8.5 International Conference, EGOV 2015, Thessaloniki, Greece, August 30 -- September 2, 2015, Proceedings* (págs. 273-290). Springer International Publishing. doi:10.1007/978-3-319-22479-4_21

Leitold, H. (2010). Challenges of eID Interoperability: The STORK Project. En S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang, *Privacy and Identity Management for Life. 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010* (págs. 144-150). Springer-Verlag Berlin Heidelberg.

Leitold, H., & Zwatterndorfer, B. (2010). STORK: Architecture, Implementation and Pilots. *ISSE 2010 Securing Electronic Business Processes* (págs. 131-142). Vieweg+Teubner.

Leitold, H., Lioy, A., & Ribeiro, C. (2014). STORK 2.0: Breaking New Grounds on eID and Mandates. *Proceedings of ID World International Congress.* Obtenido de https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=81827

Majava, J., Biasiol, A., & van der Maren, A. (2007). *eID Interoperability for PEGS. Report on comparison and assessment of eID management solutions interoperability.* European Communities. Obtenido de http://ec.europa.eu/idabc/en/document/6484/5938/

Olnes, J. (2001). A Taxonomy for Trusted Services. In B. Schmid, K. Stanoevska Slabeva, & V. Tschammer (Eds.), *Towards the E-Society: E-Commerce, E-Business, and E-Government* (Vol. 74, pp. 31-44). Kluwer Academic Publishers.

Rundle, M., Blakley, B., Broberg, J., Nadalin, A., Olds, D., Ruddy, M., . . . Trevithick, P. (2007). At a crossroads: "personhood" and digital identity in the information society. STI Working Paper 2007/07. Organisation for Economic Co-operation and Development. Obtenido de http://www.oecd.org/sti/working-papers

STORK 2.0 Consortium. (2015). *STORK 2.0. D4.8 Final version of process flows.* Obtenido de https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=56:d48-final-version-of-process-flows&Itemid=174

STORK-eID Consortium. (2011). *Secure Electronic Identity Across Europe. STORK Fact Sheet.* Obtenido de https://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=1831

Annex: Detailed list of legal requirements

Legal area	Requirement
eID	The applicant must be aware of the terms and conditions related to the use of the electronic identification means
eID	The applicant must be aware of recommended security precautions related to the electronic identification means
eID	The applicant must collect the relevant identity data required for identity proofing and verification
eID	The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid
eID	It must be known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same
eID	One of the following alternatives will be selected: a) The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity; and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person; and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence. b) An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it; and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents; c. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council (1) or by an equivalent body;

	d. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.
eID	The electronic identification means characteristics will assure that it utilises at least two authentication factors from different categories and that it is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.
eID	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs
eID	It must be possible to suspend and/or revoke an electronic identification means in a timely and effective manner
eID	There must exist measures taken to prevent unauthorised suspension, revocation and/or reactivation
eID	Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met
eID	Renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level
eID	The release of person identification data must be preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication
eID	Where person identification data is stored as part of the authentication mechanism, that information must be secured in order to protect against loss and against compromise, including analysis offline
eID	The authentication mechanism must implement security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms
eID	Providers must comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be

	retained and for how long
eID	Providers must be able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services
eID	Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.
eID	Electronic identification schemes not constituted by national law shall have in place an effective termination plan that shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.
eID	There must exist a published service definition that includes all applicable terms, privacy police, conditions, fees and any limitations of its usage
eID	Users must be informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service
eID	Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information
eID	There must be an effective information security management system for the management and control of information security risks, that adheres to proven standards or principles for the management and control of information security risks
eID	The provider must record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention
eID	The provider must retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed
eID	There must exist procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil
eID	There must exist sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures
eID	Facilities used for providing the service must be continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors

	that may impact the security of the service
eID	Facilities used for providing the service must ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors
eID	There must exist proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed
eID	Electronic communication channels used to exchange personal or sensitive information must be protected against eavesdropping, manipulation and replay
eID	Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, must be restricted to the roles and applications strictly requiring access
eID	It shall be ensured that sensitive cryptographic material is never persistently stored in plain text and is protected from tampering
eID	There must be procedures to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches
eID	All media containing personal, cryptographic or other sensitive information must be stored, transported and disposed of in a safe and secure manner
eID	There must exist periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy
Electronic signature	The device used to create the ARIES derived identity will be considered as an electronic signature creation device, having the capability of producing an advanced electronic signature
Electronic signature	The advanced electronic signature will uniquely be linked to the signatory; it will be capable of identifying the signatory; it will be created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and it will be linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
Electronic signature	The advanced electronic signature will necessarily be based in a qualified certificate for electronic signature
Electronic signature	The qualified certificate for electronic signature will necessarily be issued by a qualified trust service provider with proper qualification as a Certification Authority. The ARIES provider will therefore need to obtain the qualification
Electronic signature	The qualified certificate for electronic signature will necessarily identity the signatory by using a pseudonym, corresponding to the derived identity
Electronic signature	The qualified certificate for electronic signature will contain

	additional attributes representing any other derived identity data
Electronic signature	The ARIES provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.
Electronic signature	This information related to the identity and attributes shall be verified by the ARIES provider either directly or by relying on a third party in accordance with national law: (a) by the physical presence of the natural person or of an authorised representative of the legal person; or (b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 of the eIDAS Regulation with regard to the assurance levels 'substantial' or 'high'; or (c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal
Electronic signature	The ARIES provider shall inform the supervisory body of any change in the provision of it qualified certification service and an intention to cease those activities
Electronic signature	The ARIES provider shall employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards
Electronic signature	The ARIES provider shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law
Electronic signature	Before entering into a contractual relationship, the ARIES provider shall inform, in a clear and comprehensive manner, any person seeking to use the service of the precise terms and conditions regarding the use of that service, including any limitations on its use
Electronic signature	The ARIES provider shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them
Electronic signature	The ARIES provider shall use trustworthy systems to store data provided to it, in a verifiable form so that: (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained; (ii) only authorised persons can make entries and changes to the stored data; (iii) the data can be checked for authenticity

Electronic signature	The ARIES provider shall take appropriate measures against forgery and theft of data
Electronic signature	The ARIES provider shall record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically
Electronic signature	The ARIES provider shall have an up-to-date termination plan to ensure continuity of service
Electronic signature	The ARIES provider shall establish and keep updated a certificate database
Electronic signature	The ARIES provider shall register the revocation of a qualified certificate in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication
Electronic signature	The ARIES provider shall provide to any relying party information on the validity or revocation status of qualified certificates issued by it. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient
Electronic signature	The ARIES provider shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust service it provides. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents
Electronic signature	The ARIES provider shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein
Electronic signature	Where the breach of security or loss of integrity is likely to adversely affect the signatory, the ARIES provider shall also notify the signatory of the breach of security or loss of integrity without undue delay
Electronic signature	Where the ARIES provider, without qualified status, intends to

	start providing qualified certificated, it shall submit to the competent national supervisory body a notification of its intention together with a conformity assessment report issued by a conformity assessment body
Electronic signature	The ARIES provider will begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in the eIDAS Regulation
Electronic signature	The ARIES provider shall be audited at its own expense at least every 24 months by a conformity assessment body in order to confirm that the ARIES provider and the qualified trust service provided by it fulfil the requirements laid down in the eIDAS Regulation
Electronic signature	After the qualified status referred to in the eIDAS Regulation has been indicated in the trusted list the ARIES provider will be able to use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services it provides
Electronic signature	When using the EU trust mark for the qualified trust service, the ARIES provider shall ensure that a link to the relevant trusted list is made available on its website
Electronic signature	Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities
Electronic signature	The ARIES provider shall duly inform its customers in advance of the limitations on the use of the service it provides. Those limitations will be recognisable to third parties
GDPR	The ARIES provider shall make an inventory of all the specific purposes for which personal data are going to be processed by ARIES
GDPR	Personal data can only be linked to a concrete user during the period required by those purposes
GDPR	The users have to be informed about a. the identity and the contact details of the controller and, where applicable, of the controller's representative; b. the identity of the potential recipients to whom the personal data will be disclosed, including law enforcement agencies; c. the contact details of the data protection officer; d. the recipients or categories of recipients of the personal data; e. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; f. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as

	the right to data portability; g. the right to lodge a complaint with a supervisory authority; h. that the provision of personal data is a requirement necessary to enter into a contract; i. that the data subject is obliged to provide the required personal data to gain access to ARIES services; j. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
GDPR	The use of biometric data requires the explicit consent of the data subject for identification purposes
GDPR	The consent must be recorded in a proper way in order to answer a user's claim or to face an inspection from a supervisory authority
GDPR	A way for withdrawing their consent has to be offered to the users and the date of this action has to be registered. The withdrawal procedure has to be as easier as giving the consent
GDPR	A concise, transparent, intelligible and easily accessible form, using clear and plain language, shall be offered by the AIRES provider in order to allow users to exercise their rights to access, to rectification inaccurate data concerning them, to erasure their data when a legal provision applies, to restriction of processing them
GDPR	The ARIES provider must allow users' access to their own data in a structured, commonly used and machine-readable format
GDPR	The ARIES provider shall create a record of processing activities. This record has to adopt the adequate security measures for storing and processing users´ personal data taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons
GDPR	When the linkage of data with the identity of the user is not indispensable pseudonymisation criteria should be applied to the processing operations. Nevertheless, there must be a way to re-identify the user in order to make the information available to a competent public authority
GDPR	By default, only personal data necessary for each specific purpose can be used processed by the ARIES provider and other users. This requirement not only has to be applied to the amount of personal data collected, but to the extent of their processing, the period of their storage and their accessibility as well
GDPR	For the airport scenario, the use of Passenger Name Record (PNR) must be restricted to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes

Law enforcement	The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require ARIES to comply with any request of information about the users' activity
Law enforcement	The consent of users is not necessary for this purpose although they must be informed about this data processing when signing up the ARIES system
Law enforcement	The ARIES provider must give access to the users' data stored in the Secure Vault when it is necessary for the performance of a task carried out by a law enforcement agency. The access will be subjected to the legal framework of the Member State where it is established
Law enforcement	When a different Member State law enforcement agency needs to obtain information from the Secure Vault a direct access will not be allowed. It will have to obtain those data through the official procedures fixed by the EU mechanism and protocols
Law enforcement	The requests for disclosure sent by law enforcement authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems
Law enforcement	The ARIES interface shall implement secure communication, strong authentication and authorization mechanisms, and enable the law enforcement agency to retrieve requested information among the different transactions on READ-ONLY basis. All the requests will be logged to keep the full history of investigation events
Law enforcement	The ARIES interface should inform the law enforcement authority that the data obtained cannot be processed for purposes incompatible with those related to prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
Law enforcement	The AIRES provider might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings and is obliged to provide information on criminal offences
Consumer rights	The ARIES provider shall provide the consumer with the information required by Consumer rights Directive in a clear and comprehensible manner
Consumer rights	The ARIES provider shall give the information about qualified certificate for electronic signature or make that information available to the consumer in a way appropriate to the means of distance communication used in plain and intelligible language. In so far as that information is provided on a durable medium, it shall be legible
Consumer rights	If the contract is concluded through a means of distance

	communication which allows limited space or time to display the information, the ARIES provider shall provide, on that particular means prior to the conclusion of such a contract, at least the pre-contractual information regarding the main characteristics of the service, the identity of the ARIES provider, the total price, the right of withdrawal, the duration of the contract and, if the contract is of indeterminate duration, the conditions for terminating the contract
Consumer rights	The ARIES provider shall provide the consumer with the confirmation of the contract concluded, on a durable medium within a reasonable time after the conclusion of the distance contract, and at the latest before the performance of the service begins
Consumer rights	Where a consumer wants the performance of services to begin during the withdrawal period, the ARIES provider shall require that the consumer make an express request
Consumer rights	The consumer shall have a period of 14 days to withdraw from a distance or off-premises contract, without giving any reason, and without incurring any costs other than those provided for in Article 13(2) and Article 14 of the Consumer rights Directive. The withdrawal period shall expire after 14 days from the day of the conclusion of the contract.
Consumer rights	The ARIES provider shall reimburse all payments received from the consumer, including, if applicable, the costs of delivery without undue delay and in any event not later than 14 days from the day on which he is informed of the consumer's decision to withdraw from the contract
Consumer rights	The ARIES provider shall not charge consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the ARIES provider for the use of such means
Information society services	The ARIES provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities the information required by the e-commerce Directive
Information society services	Where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs
Information society services	Commercial communications performed by the ARIES provider shall comply at least with the following conditions: a. the commercial communication shall be clearly identifiable as such; b. the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable; c. promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly

	identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously
Information society services	The ARIES provider shall not send unsolicited commercial communications unless it is permitted by the ARIES provider applicable national law. If allowed, such commercial communication shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient
Information society services	The ARIES provider undertaking unsolicited commercial communications by electronic mail shall consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves, according to the ARIES provider applicable national law
Information society services	The ARIES provider service shall give the following information, clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service: a. the different technical steps to follow to conclude the contract; b. whether or not the concluded contract will be filed by the service provider and whether it will be accessible; c. the technical means for identifying and correcting input errors prior to the placing of the order; d. the languages offered for the conclusion of the contract
Information society services	Contract terms and general conditions provided by the ARIES provider to the recipient must be made available in a way that allows him to store and reproduce them
Information Society Services	The ARIES service provider shall make available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order. The ARIES provider shall acknowledge the receipt of the recipient's order without undue delay and by electronic means. The order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them