002374-6000413905-REQ-01 DIGIT B.1/STIS III

ISA Action 1.18 Consolidation Report

Deliverable

Reference: STIS III-002374-6000413905-REQ-01

Framework contract: STIS III framework

Version 1.0

September 2016

Document Metadata

Property	Value
Release date	08/09/2016
Status:	*Final*
Version:	*1.0*
Authors:	*Marta Alberto Monferrer* *John Heppe* *Joan Costa Sintes*
Reviewed by:	*Alice Vasilescu*
Approved by:	*Alice Vasilescu*

Document History

Version	Date	Description	Action
0.1	23/02/2016	Table of contents	Creation
0.2	17/05/2016	Introduction of contents: sections 1 to 10, except section 8 (Recommended solution)	Overall document writing except section 8 (Recommended solution)
0.3	05/07/2016	Review of pros/cons of each potential solution. Integration of the EC comments and the insights gathered from the meetings. Introduction of contents to section: ANNEX III – Meetings. Integration of feedback received during the Second Workshop	Overall document review and introduction of missing contents
0.4	05/09/2016	Reviewed according EC comments received on 23/08/2016	Review of sections 6.7.1, 7.2.3.1, 7.2.3.2, 7.2.5, 7.2.6; and chapter 8.

1.0	08/09/2016	Preparation of final release without comments and track changes	Preparation of final release

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Context

This document has been created in the context of **Phase 3** of **ISA Action 1.18** [1]. Action 1.18 stands for Federated Authorisation across European Public Administrations. The objective of Action 1.18 is to extend European Commission Authentication Service (**ECAS**) multi-factor authentication using **STORK** (Secure idenTity acrOss boRders linKed) with a federated authorisation solution that allows public officials to log in to European Commission (EC) applications and be granted access based on their role or position in a national administration.

The ECAS-STORK integration provides a high level of assurance regarding the identity of citizens and promotes **EU-wide interoperability of electronic identities (eID)**. Hence, Action 1.18 is placed within the ISA programme [2] objectives of establishment and improvement of common frameworks in support of interoperability across borders and sectors.

The objective of Phase 3 is to review and consolidate the different federated authentication approaches undertaken within the context of STORK related projects and to propose the way to integrate the authorisation to access EC applications, the objective of this action, in STORK and CEF/eIDAS reference projects.

1.2 Objective of this Document and Intended Audience

The objective of this document is to consolidate the analysis conducted throughout Phase 3 of ISA Action 1.18. This consolidation is achieved through the analysis of the relevant environment, the proposal of potential solutions and a final recommendation for the federated authorisation solution.

The relevant environment that may influence the potential solutions, both from the technical and governance perspectives, has been studied. The analysis includes driving elements such as: the legal context with eIDAS as flagship regulation, the implementation options specified by relevant state-of-the-art standards, the approaches undertaken in the context of STORK related projects and the emerging eIDAS eID infrastructure.

The consolidation outcome consists of a set of potential solutions and a final recommendation for the federated authorisation. These solutions must be based on the ECAS and STORK/eIDAS integration as required by the objectives of ISA Action 1.18.

This document is addressed to the ISA Programme, ISA SEMIC expert group, Member States representatives, and the Project Management Board of the ISA Action 1.18 to support their decisions concerning the federated authorisation solution across European Public Administrations.

1.3 Overview of the Document

This document consists of the following chapters:

- Chapter 1: **Introduction**, describes the objective of this document and how it fits into ISA Action 1.18.
- Chapter 2: **Approach** for the consolidation of this document, describes the methodological approach defined for the analysis and consolidation of the different solutions from both the technical and governance perspectives.
- Chapter 3: **Legal** Environment, focuses on the analysis of the legal environment, detailing the most influential characteristics and requirements applicable to the solution to be proposed.
- Chapter 4: **Application of Standards**, outlines the technical alternatives on the basis of the features provided by the relevant state-of-the-art standards, and their implementation integrated with the STORK/eIDAS architecture.
- Chapter 5: Analysis of **Reference Projects**, examines the projects which have established or are establishing an eID interoperability platform, implemented in several MS (e.g. STORK) or in all MS (e.g. CEF-eID/eIDAS). The solution to be proposed in this analysis should be integrated in this solution. The analysis details the most influential characteristics and findings.
- Chapter 6: Analysis of **Domain Specific Projects**, analyses domain specific projects that, at some point, have implemented or reused a federated eID solution, detailing the most influential characteristics and findings, especially their experiences with such federated solutions.
- Chapter 7: **Potential Solutions**, describes the most evident potential solutions for federated authorisation which fit into the requirements that have emerged from the previous analysis, including governance and technical details along with their advantages and drawbacks.
- Chapter 8: **Recommended Solution**, describes the final recommended solution in detail. This chapter elaborates on the selection rationale and the solution.
- Chapter 9: **Conclusions and Next Steps**, describes the most important conclusions of this study, apart from the recommended solution, as well as a recommendation for the subsequent steps to be undertaken.
- ANNEX I: Summarizes of the **history of solutions** in the context of ISA Action 1.18.
- ANNEX II: Contains the **Acronyms** and **Bibliographical References**.
- ANNEX III: Contains the list of **Meetings** held during the project.

2 Approach for the Consolidation

This section describes the methodology applied to elaborate this document. The methodology comprises of the following steps:

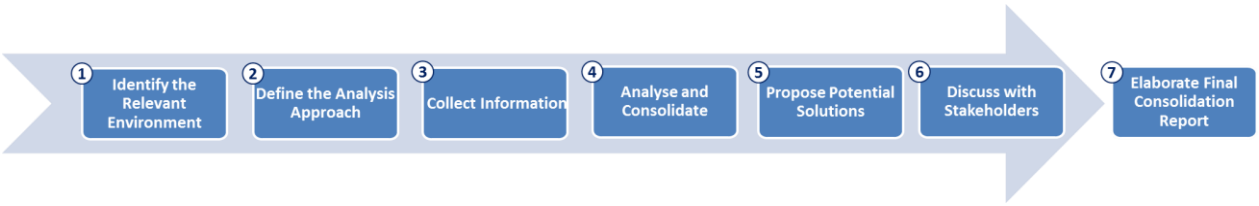


Figure 1: Methodological approach for the elaboration of this document

The goal of each step is briefly summarised below:

1. **Identify the Relevant Environment**. From the beginning it was foreseen that the environment that influences the federated authorisation was broad, complex and comprised of different domains. In this step, an identification of the categories of such relevant environment was conducted. See Section 2.1 for more details.
2. **Define the Analysis Approach**. In order to narrow the analysis, and conduct an efficient study, it was necessary to specify the **characteristics to be analysed**. The characteristics of each category are not coincident because they belong to different domains. Moreover, the principal **fields of influence** on the potential federated authorisation solutions were specified. See Section 2.2 for more details.
3. **Collect Information**. Desk research and interviews were conducted to gather all the necessary information and understanding of the relevant environment. See Section 0 for more details.
4. **Analyse and Consolidate**. On the basis of the information gathered, an analysis was conducted to synthesise the major findings and consolidate them into requirements, recommendations and potential solutions. See Section 2.4 for more details.
5. **Propose Potential Solutions**. The potential solutions that emerged from the previous step are described in detail in this step, providing technical and governance insights along with their advantages and drawbacks for later discussion in the Second Workshop. See Section 2.5 for more details.
6. **Discuss with Stakeholders**. A short-list of the potential solutions will be discussed during the Second Workshop in order to agree on the most convenient solution. See section 2.6 for more details.
7. **Elaborate Final Consolidation Report**. Lastly, the feedback and recommendations gathered during the Workshop will be integrated in this document in order to conclude the final consolidation report with a recommended solution. See section 2.7 for more details.

The following sections detail each step of the methodology.

2.1 Identify the Relevant Environment

A preliminary analysis revealed that the relevant environment of federated authorisation is broad, complex and comprises different domains.

Many relevant references have been identified as driving elements for the technical and governance perspectives of the potential solutions. These references have been grouped into **four categories of relevant environment**: Legal, Standards and Open Initiatives, Reference Projects and Domain Specific Projects.

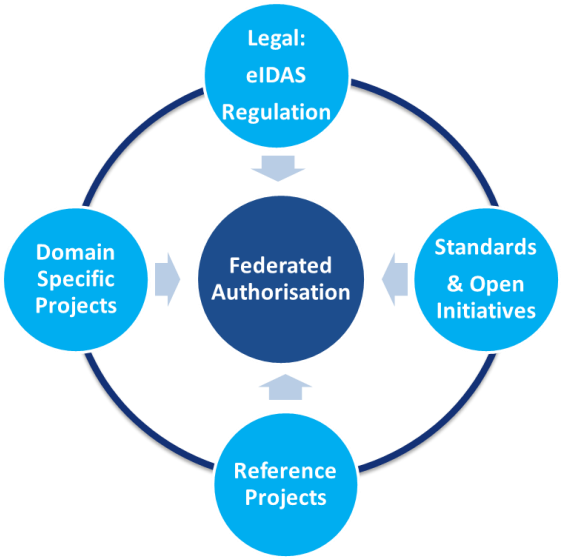
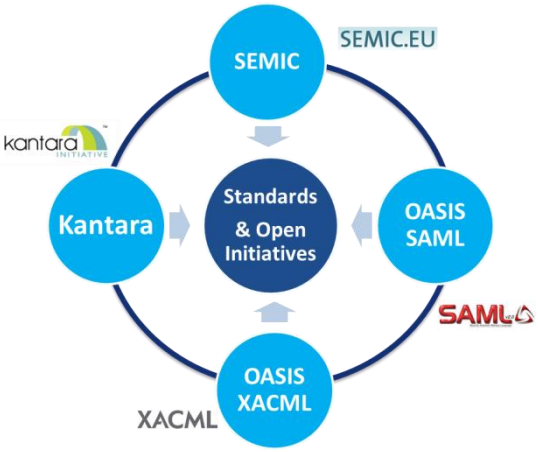


Figure 2: Relevant Environment of federated authorisation

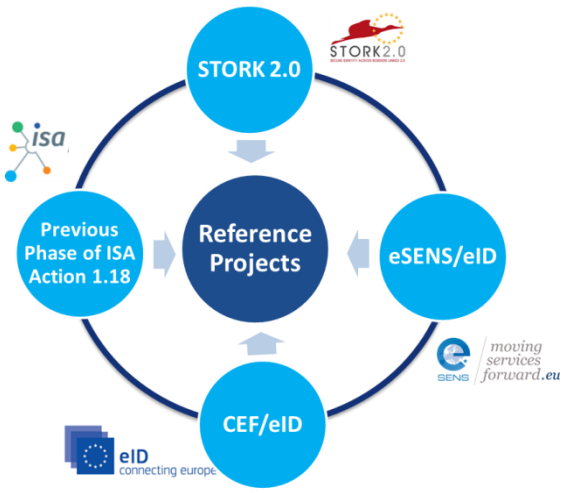
A description of each relevant environment category and its sub-elements is provided below:

- **Legal**. The recently approved eIDAS Regulation [3] is the first item of this category. The analysis also includes related implementation acts and privacy directives. The analysis details are included in Chapter 3 of this document.
- **Standards and Open Initiatives**. The solution proposed in this study needs to be sustainable, so one of the mandatory principles to apply is the compliance of standards. The most relevant standards have been elaborated by the OASIS group: **SAML** [4] and **XACML** [5]. In addition to the standard SAML specification per se, another SAML variant is considered: the one elaborated by the **Kantara Initiative** group. At a European level, the **SEMIC** [6] standard definition work on **Core Vocabularies** [7] is analysed because the eIDAS minimum data sets can be derived from



SEMIC Person and Business Core Vocabularies. On the basis of these SEMIC Core Vocabularies, the eIDAS Technical Sub-group has developed the **eIDAS SAML Attribute Profile** specification [8]. The analysis details are included in Chapter 4 of this document.

- **Reference Projects**. In the last few years, several European initiatives for the implementation of a common cross-border eID platform have been developed, into which the solution is to be integrated. Some of these initiatives for cross-border eID are currently operational. Others will be operational within a short time-frame. Initially, the **STORK** / **STORK 2.0** [9] projects established the eID European interoperability platform between 19 European Member States (MS). STORK was also connected to the ECAS system. Then, when the STORK 2.0 project ended, the responsibility for maintenance and improvement of its common specifications and code was transferred to the **e-SENS** [10] project, within its eID building block.

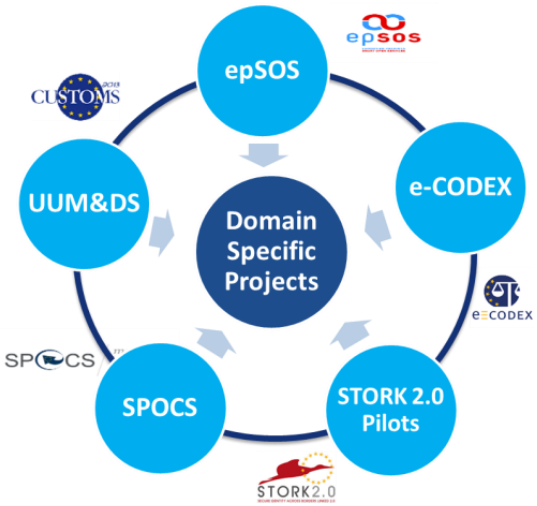


Finally, all Member States have the obligation to establish their eIDAS node before September 2018. In order to facilitate the compliance of this obligation, the EC has published, within the **CEF**/eID programme, a common code based on the eIDAS specifications.

In addition, the work performed in the Previous Phase of ISA Action 1.18 is analysed in this chapter, as the experience from this phase has revealed similar lessons learned to other reference projects.

The analysis details of these projects are included in Chapter 5 of this document.

- **Domain Specific Projects**. At the same time, some domain oriented European projects had to deal with cross-border authentication and authorisation requirements as well. Their approaches and experience to cross-border eID and authorisation mechanisms are analysed. Most of these projects are maintained and evolved by e-SENS in order to provide a common EU platform of reusable services. The analysis details are included in Chapter 6 of this document. A summary of their relevance is detailed below:
    - **epSOS** achieved the cross-border interoperability of health data allowing



patients to consult their medical records while being in another country.

- **SPOCS** built the next generation of online portals through cross-border electronic procedures.
- **e-CODEX** improved the cross-border access of citizens and businesses to legal means in Europe as well as the interoperability between legal authorities within the EU.
- **UUM&DS**. This Uniform User Management & Digital Signatures project specifies a secure authorised interface for EU economic operators, facilitating cross-border access to central customs information systems. UUM&DS also specifies an authorisation mechanism.
- **STORK 2.0 pilot 3 (eGov4Business)** has used the common STORK eID infrastructure to establish services of opening a foreign branch office by a company, interrogating connected business registers for legal person's data as well as the powers of representation the user has on behalf of this legal person.
- **STORK 2.0 pilot 4 (eHealth)** used the common STORK eID infrastructure to establish services for consulting a patient's medical file by implementing 3 use-cases: 1) by himself, using his eID; 2) by the qualified HealthCare Professional through a role based authorisation; and, by 3) other persons, after obtaining the patient's mandate.

2.2 Define the Analysis Approach

In order to narrow the analysis, conduct an efficient study and consolidate the amount of information gathered, it was necessary to specify the **characteristics** that should be analysed for each of the categories of the relevant environment. A vast amount of information was available for most of the relevant environment to analyse. Thus the overall approach was only to focus on the functional/semantic, technical and governance topics related to federated eID and authorisation.

The final selection of characteristics depended on the domain of the category itself and its foreseeable influence in the potential solutions specification.

Moreover, it was necessary to define "how" they can "influence" the specification of the potential federated authorisation solutions. Thus, a set of **fields of influence** were identified which drove such specification. As mentioned before, the functional/semantic, technical and governance related topics are mandatory concerns to be considered along with the analysis.

The following table summarises the analysis approach:

Environment	Characteristics to Analyse	Fields of Influence
Legal	Article-by-article and implementation acts	Requirements
Standards & Open Initiatives	Summary of the standards and their technical applicability	Technical alternatives of the eID solution

Environment	Characteristics to Analyse	Fields of Influence
Reference Projects	Technical, Functional, EU environment, Governance, Outcome, Sustainability	Requirements, eID solution, Governance, Recommendations
Domain Specific Projects	Technical, EU Environment, Outcome, Sustainability	Experiences, Recommendations

Table 1. Mapping of the environment analysed and its fields of influence

2.3 Collect Information

To collect the necessary information for the analysis, the following actions were conducted:

- An initial workshop was held on 9th February 2016 with the ISA Action 1.18 stakeholders. The objective was to introduce the goal for Phase 3, to agree on the approach for the elaboration of the consolidation report and to enlist their collaboration in the study.
- Extensive desk research was performed based on public documentation available online from the projects, organisations, initiatives and standards identified in the Relevant Environment.
- Various teleconferences were held with the different stakeholders to improve the understanding of some characteristics and the expectations for the near future. The stakeholders interviewed represented the following organisations: SEMIC, UUM&DS, e-SENS/eID WP6, e-SENS/Adaptor STORK development, e-SENS/eID MS, eIDAS dataset, and OASIS.

The information collected was summarised in its corresponding chapter according to its environment category: Legal (Chapter 3), Standards and Open Initiatives (Chapter 4), Reference Projects (Chapter 5), and Domain Specific Projects (Chapter 6).

2.4 Analyse and Consolidate

On the basis of the information gathered, an analysis was conducted to synthesise the major findings and consolidate them into recommendations and potential solutions.

This consolidation was driven by the fields of influence specified in the methodological approach.

2.5 Propose Potential Solutions

The potential solutions that emerged from the “Analysis and Consolidation” step are described in detail in a specific section for this purpose (see Chapter 7).

The description included not only presents details for each technical option and governance recommendations, but also the advantages and drawbacks for later discussion in the Second Workshop.

The Second Workshop has been held on the 22th of June 2016. During the workshop, an extract draft of this document has been shared with the stakeholders in presentation format.

2.6 Discuss with Stakeholders

During the Second Workshop, the list of potential solutions has been discussed in order to agree on the proposed solutions and its benefits and disadvantages. The results of the discussion are reflected in Chapter 8.

2.7 Elaborate Final Consolidation Report

In addition to the analysis and outcome of the previous steps, the conclusions of the Second Workshop have been integrated into the final consolidation report, which is actually this document.

Sections 8 and 9 are concluded during this final step.

3 Legal Environment

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" [3], is commonly known as **the eIDAS Regulation,** or simply **The Regulation**.

This Regulation, as mentioned in its point 2 of the considerations ("whereas"), "seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the European Union."

Whereas the Regulation **establishes the legal framework for mutual acceptance of European credentials**, its implementation acts and technical specifications [11] establish the organisation and technical requirements for this acceptance. Of the Regulation, chapter II, on Electronic identification, is analysed together with the implementation acts. The technical specifications are analysed in section 5.3, as they are implemented under the CEF/eID framework, which is the reference eIDAS platform. Since the STORK project timeline was prior to the eIDAS Regulation, STORK per se is not compliant with eIDAS, but e-SENS is currently developing an eIDAS adaptor for the STORK nodes.

The following sections analyse the relevant aspects in order to identify the **requirements imposed** by the Regulation. The requirements derived from this Chapter are catalogued in Chapter 7 of this document.

The **Electronic Identification** chapter of the Regulation is analysed in depth because it contributes to the analysis with the most relevant aspects. The rest of the Regulation has been reviewed, but no relevant requirements have been found.

Thus, on the next sections the following legal environment is analysed:

- The data protection directive.
- The eIDAS Regulation.
- The eIDAS Implementing act (EU) 2015/296.
- The eIDAS Implementing act (EU) 2015/1501.
- The eIDAS Implementing act (EU) 2015/1502.

3.1 Data protection directive

Description: The protection of personal data is a worry for many EU citizens. This is the reason why the Commission has issued the data protection directive 95/46/EC. The Regulation emphasises the requirement of compliance of this directive with the statement, "Processing of personal data shall be carried out in accordance with Directive 95/46/EC".

Impact: As the solution to be proposed will be embedded in the CEF/eIDAS and STORK platforms, which are respectful of this requirement, this requirement will be fulfilled.

3.2 The Regulation

3.2.1 Mutual recognition

Description: The Regulation 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 the following conditions are met: […]. Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first sub-paragraph".

Impact: Such mutual recognition is to be implemented by most eGovernment portals, and doesn't affect the authorisation when accessing EC applications. Thus, this article does not impose any requirement on the federated authorisation solution.

3.2.2 Eligibility for notification of electronic identification schemes

Description: The Regulation states that "An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met: […]".

Impact: Such identification schemes are to be implemented by eIDAS eIdentification services, and don't affect the authorisation when accessing EC applications. However, the quality of the authentication, which depends on the identification scheme, may affect the acceptance of the credential, and as a consequence the acceptance of the authorisation. This article does not impose any requirement on the federated authorisation solution.

3.2.3 Assurance levels of electronic identification schemes

Description: The Regulation states that "An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme." And "The assurance levels low, substantial and high shall meet respectively the following criteria: […]".

Impact: Such assurance levels are implemented by notified eIdentification services, and in principle, don't affect the authorisation when accessing EC applications. The EC application owners should be aware that the required assurance level may cause the failure of the authentication, and as a consequence, of the authorisation. This article does not impose any requirement on the federated authorisation solution.

3.2.4 Notification

Description: The Regulation states that "The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto: […]".

Impact: Such notification is performed by Member States, and doesn't affect the authorisation when accessing EC applications. Thus, this article does not impose any requirement on the federated authorisation solution.

3.2.5 Security breach

Description: The Regulation states that "Where either the electronic identification scheme notified pursuant […] or the authentication […] is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission. […]".

Impact: Such suspension or revocation is performed by Member States, and doesn't affect the authorisation when accessing EC applications. However, it is important that security breaches are detected, notified and that measures are taken as soon as possible, in order to limit the unreliable information, e.g. revocation of the signing certificate of the eIDAS node. Anyway, this article does not impose any requirement on the federated authorisation solution.

3.2.6 Liability

Description: The Regulation states that "The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations […] in a cross-border transaction". And "The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation […] in a cross- border transaction. […]".

Impact: Such liability is assumed by Member States and their identity providers, and is a guarantee for the authorisation when accessing EC applications. But, this article does not impose any requirement on the federated authorisation solution.

3.2.7 Cooperation and interoperability

Description: The Regulation states that "The national electronic identification schemes notified […] shall be interoperable. For the purposes of paragraph 1, an interoperability framework shall be established". And "Member States shall cooperate with regard to the following: […]".

Impact: Such cooperation is performed by the Member States and benefits the authorisation to access EC applications. But this article does not impose any requirement on the federated authorisation solution.

3.2.7.1 Criteria for the interoperability framework

Description: The interoperability framework shall meet the following criteria:

- It aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State.
- It follows European and international standards, where possible.
- It facilitates the implementation of the principle of privacy by design.
- It ensures that personal data is processed in accordance with Directive 95/46/EC.

Impact: The solution proposed in this document needs to meet these requirements.

3.2.7.2 Components of the framework

Description: The interoperability framework shall consist of:

- a reference to minimum technical requirements related to the assurance levels under Article 8;
- a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;
- a reference to minimum technical requirements for interoperability;
- a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;
- rules of procedure;
- arrangements for dispute resolution; and
- common operational security standards.

Impact: The solution proposed in this document needs to meet the requirements of the framework. However, the components of the framework are requirements for the eIDAS platform, within which the solution for federated authorisation is to be integrated, not for the solution itself.

3.2.8 Commission Implementing Decision (EU) 2015/296

Description: "establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation."

Impact: It is important that the cooperation between Member States is organised. This cooperation could be relevant for possible solutions regarding sustainability.

3.2.9 Commission Implementing Regulation (EU) 2015/1501

Description: "on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014."

Impact: It is important that the technical and operational requirements of the interoperability framework are laid down, in order to ensure the interoperability of the electronic identification schemes.

3.2.10 Commission Implementing Regulation (EU) 2015/1502

Description: “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.”

Impact: It is important that the quality of authentication schemes is established.

3.2.11 Commission Implementing Decision (EU) 2015/1984

Description: “defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014.”

Impact: It is important that the circumstances, formats and procedures of notifications of electronic identification schemes to the Commission are laid down.

4 Application of Standards and Open Initiatives

4.1 Introduction

This chapter analyses the relevant environment related to standards and open initiatives. For each element analysed, the following sections are provided: 1) a summary and 2) the description of the applicability of such standards as potential solutions.

As stated earlier, one of the mandatory principles to apply to the solution is the compliance to standards. The analysis in this section starts with SEMIC, which specifies Core Vocabularies that are candidates to be considered. It then continues with OASIS relevant standards (SAML and XACML), and ends with Kantara that has developed a profile based on SAML.

4.2 SEMIC (ISA² initiative)

4.2.1 Summary of the initiative

The Semantic Interoperability Community (SEMIC) [6] is a European Commission initiative aimed at improving the **semantic interoperability** of interconnected e-Government systems.

Semantic interoperability refers to the preservation of meaning in the exchange of electronic information in such a way that, in the context of an information exchange, the receiver and the sender of information can understand and interpret it the same way.

To this end, SEMIC works on several initiatives. However, the analysis focuses only on the initiatives that may impact the potential federated authorisation solution(s): Core Vocabularies [7] and Community of Practice [12] of data standards.

On one hand, the **Core Vocabularies** initiative defines simplified, re-usable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral and syntax-neutral fashion. As such, the Core Vocabularies are promoted as cross-sector semantic building blocks. The Core Vocabularies are introduced hereafter:

- **Person**: fundamental characteristics of a person, e.g. the name, the date of birth, etc.
- **Business**: fundamental characteristics of a legal entity, e.g. the legal name, the activity, etc.
- **Public Service**: fundamental characteristics of a service offered by public administration, e.g. title, description, inputs, outputs, providers, locations, etc.
- **Location**: fundamental characteristics of a location, represented as an address, a geographic name or a geometry.

On the other hand, the **Community of Practice** works on specifications, good practices and lessons learned for setting up proper governance and management of data standards. Therefore, it has been verified if there are some recommendations available that may be applicable to this study. However, at the time of writing, this is not the case.

4.2.2 Usage of Core Vocabularies

The Core Vocabularies can be used in any of the following ways [13]:

- Map existing data models to the Core Vocabularies.
- Design new data models that extend the Core Vocabularies. Then, the Core Vocabularies become the foundation of domain data models, which are context-specific.

Both possibilities are already embraced by SEMIC and eIDAS Technical Sub-group to fill the standardisation gap regarding the eID data set.

The first usage, mapping of existing data models to the Core Vocabularies, is already adopted by the eIDAS Technical Sub-group to specify the **eIDAS SAML Attribute Profile** [8]. This eIDAS standard profile is **based on the mapping of the eIDAS conceptual minimum dataset** [14] [15] **to the SEMIC Person and Business Core Vocabularies**. The eIDAS Technical Sub-group conducted such standard mapping and established the foundation of semantic interoperability because different systems use the same semantics to encode identity information. This eIDAS standard profile was defined in June 2015, but previously, SEMIC anticipated, internally, the convenience of conducting such mapping to maximise and reuse standardisation efforts.

The second usage, design new data models extending Core Vocabularies, provides additional meaning such as the mandate concept could supply to the new dataset. In this regard, it should be noted that the **upcoming Action of ISA²** [16], "Semantic Interoperability for Representation Powers and Mandates", plans to **provide a common data model for representation powers / mandates** linked to legal entities, **aligned with the Core Person and Core Business Vocabularies** in order to be used by eIDAS for eID. Thus, following this approach, the integration of authorisation information (e.g. mandate, role or permissions) could be done through the extension of Core Vocabularies.

4.3 OASIS SAML

4.3.1 Summary of the standard

OASIS' Security Assertion Markup Language (SAML) [17] standard is designed to support federated authentication, but also supports authorisation, and as such, seems to be an adequate candidate for the technical solution to be proposed in this document.

The support for authorisation lays in the assertion, which may contain several statements, each of which can be either an authentication, attribute or authorisation statement. This is represented by the following definition.

```
<choice minOccurs="0" maxOccurs="unbounded">
       <element ref="saml:Statement"/>
       <element ref="saml:AuthnStatement"/>
       <element ref="saml:AuthzDecisionStatement"/>
       <element ref="saml:AttributeStatement"/>
</choice>
```

However, the authorisation decision seems to be “old-fashioned”, as the OASIS documentation states in [18], section 2.7.4: “Note: The <AuthzDecisionStatement> feature has been frozen as of SAML V2.0, with no future enhancements planned. Users who require additional functionality may want to consider the eXtensible Access Control Markup Language [XACML], which offers enhanced authorisation decision features.”

Currently no initiative is being undertaken by the OASIS workgroups to eliminate this statement or to declare it obsolete.

As far as the new version of SAML 2.1 is concerned, no document has been published yet and isn’t foreseen before the finalisation of this report. As far as the OASIS’ wiki page [19] states, for many topics, there has been no progress so far. At the time of writing, the new version of SAML is not a high priority for the OASIS group.

4.3.2 Applicability of the standard

SAML is already implemented in the eIDAS and STORK nodes, so this seems relatively easy to adopt for the federated authorisation solution. The process flows are illustrated by the following diagram.

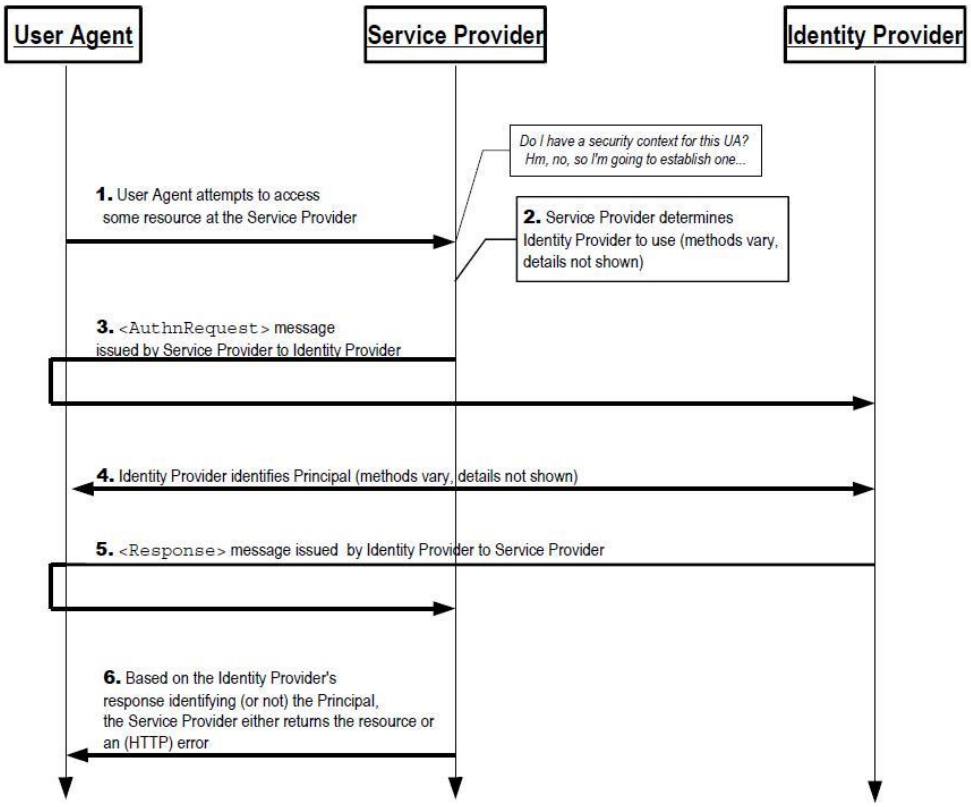


Figure 3: SAML process flows and functions in relevant systems

Within the standard SAML assertion, two implementation options concerning authorisation may be considered:

- To use the **AttributeStatement**. An attribute statement asserts that a subject is associated with certain attributes. Relying parties use attributes to make access-control decisions. The attribute could either be a Mandate or a new simple attribute of which type and name have to be defined.
- To use the **AuthzDecisionStatement**. An authorisation decision statement asserts that a subject is permitted to perform action A on resource R given evidence E. The expressiveness of authorisation decision statements in SAML is intentionally limited. More-advanced use cases are encouraged to use XACML instead.

The advantages and drawbacks of these options are discussed in Chapter 7.

4.4 OASIS XACML

4.4.1 Summary of the standard

OASIS' eXtensible Access Control Markup Language (XACML) standard [20] is designed to support federated authorisation, and as such seems to be the best candidate for the solution to be proposed in this document. XACML specifies schemas for authorisation policies and for authorisation decision requests and responses. It also specifies how to evaluate policies against requests to determine a response.

XACML specifies that a **Policy Enforcement Point** (PEP) is responsible for protecting access to one or more resources. When a resource access is attempted, the PEP sends a description of the attempted access to a **Policy Decision Point** (PDP) in the form of an authorisation decision request. The PDP evaluates this request against its available policies and attributes and produces an authorisation decision that is returned to the PEP. The PEP is responsible for enforcing the decision. The PDP may obtain policies from on-line **Policy Administration Points** (PAP) or from **Policy Repositories** into which PAPs have stored policies. The **Policy Information Point** (PIP) holds the description resources and possible access rights.

XACML defines the authorisation process flows as described in the following diagram.

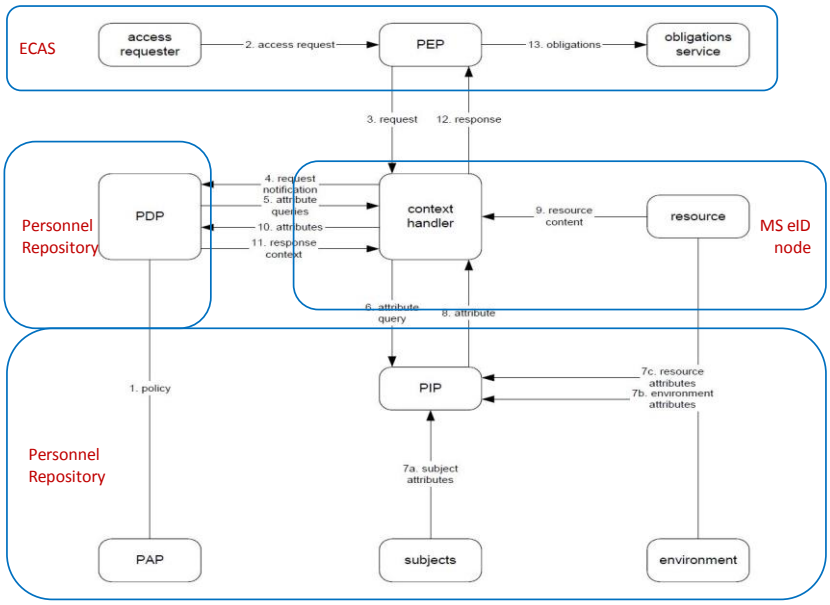


Figure 4: XACML process flows and functions in relevant systems

The model operates by the following steps.

1. The PAP writes policies and policy sets and makes them available to the PDP. These policies or policy sets represent the complete policy for a specified target.

2. The access requester sends a request for access to the PEP.

3. The PEP sends the request for access to the Context Handler in its native request format, optionally including attributes of the subjects, resource and action. The Context Handler constructs an XACML request context in accordance with steps 4, 5, 6 and 7.

4. Subject, resource and environment attributes may be requested from a Policy Information Point (PIP).

5. The PIP obtains the requested attributes.

6. The PIP returns the requested attributes to the Context Handler.

7. Optionally, the Context Handler includes the resource in the context.

8. The Context Handler sends a decision request, including the target, to the PDP. The PDP identifies the applicable policy and retrieves the required attributes and (optionally) the resource from the context handler. The PDP evaluates the policy.

9. The PDP returns the response context (including the authorisation decision) to the Context Handler.

10. The Context Handler translates the response context to the native response format of the PEP. The Context Handler returns the response to the PEP.

11. The PEP fulfils the obligations.

12. (Not shown) If access is permitted, then the PEP permits access to the resource; otherwise, it denies access.

XACML itself defines only some of the messages necessary to implement this model, but deliberately does not define protocols or transport mechanisms. Full implementation of the usage model depends on use of other standards to specify assertions, protocols, and transport mechanisms. XACML also doesn't specify how to implement a PEP, PAP, Context Handler, or repository. SAML is a suitable standard for providing the assertion and protocol mechanisms needed by XACML. In this regard, OASIS defined a SAML profile for XACML [21].

4.4.2 Applicability of the standard

Considering that XACML is not a subordinate standard to SAML as the standard is complementary, the process flows would be depicted in the following manner (see Figure 5 below):

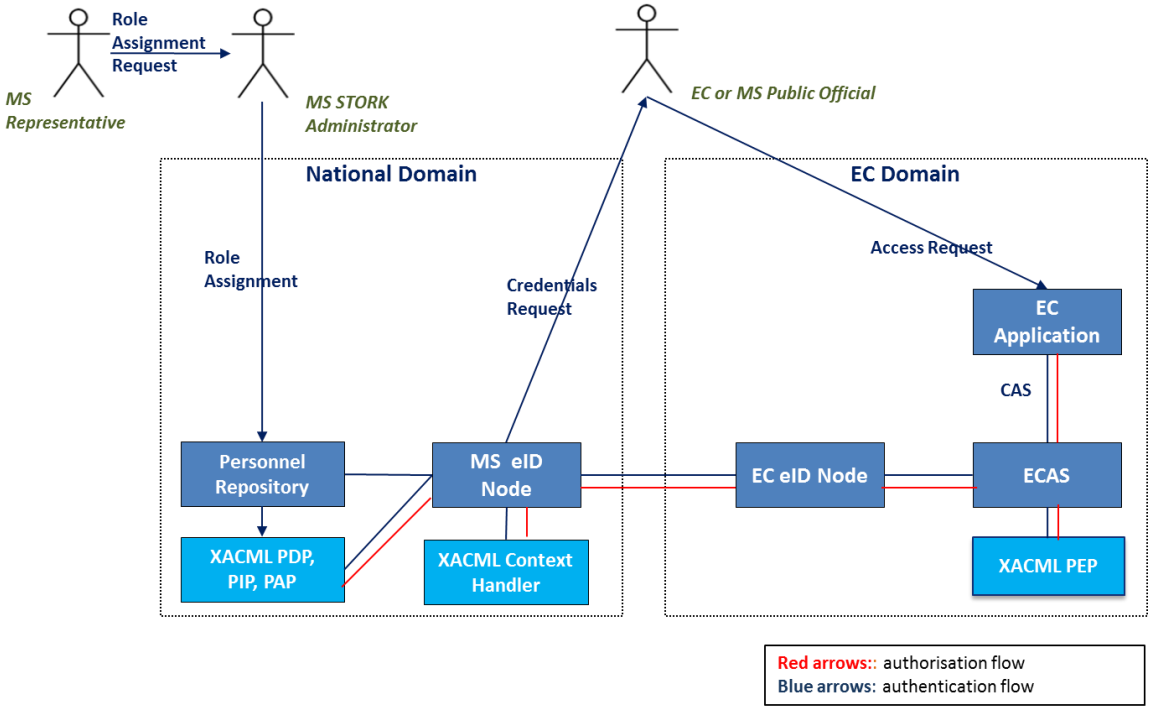


Figure 5: Projection of XACML flows and modules to ECAS integration with STORK or eIDAS

Projecting the XACML flows and modules to the relevant systems in this project, the PDP, PIP and PAP, as well as information about subjects, resources and environment would be part of the MS Personnel repository. The Context Handler and resource information should be part of the STORK/eIDAS node. ECAS should be enhanced with the PEP function, as well as the transformation of internal access requests / response to XACML requests / responses.

Independently of the dialogue between the EC application and the ECAS system, the recommended implementation would imply that ECAS would send one SAML request to the EC STORK/eIDAS node (blue arrows) for the user's identity and maintaining the session until the SSO timeout, and one XACML request for each accessed application (red arrows). This EC STORK would send these requests to the MS STORK/eIDAS node, which would then distribute them between the IDP and the personnel repository.

Of course, the communication between ECAS and the EC STORK/eIDAS node is specific, and so is the communication between the MS STORK/eIDAS node and the Personnel Repository. Each MS may determine the best solution for itself.

4.5 Kantara Initiative

4.5.1 Summary of the standard

Kantara Initiative is a business acceleration organisation that is a global, open, and transparent community stakeholder expert representing enterprise deployers, mobile operators, service providers, eGovernment agencies, IT vendors, and consumer electronics vendors.

This group has published a standard called the "Kantara Initiative eGovernment Implementation Profile of SAML V2.0" [22] as a recommendation for usage of SAML 2.0. As such, it is a blend of OASIS SAML2.0. This standard has been adopted by main software manufacturers, like IBM and Sun Microsystems (now part of Oracle).

This recommendation limits itself to authentication and possibly additional attributes, but no authorisation is described. In section "2.5.3.2 Message Content" of the referred document it states:

"The Web Browser SSO Profile allows responses to contain any number of assertions and statements. Identity Provider implementations MUST allow the number of `<saml2:Assertion>`, `<saml2:AuthnStatement>`, and `<saml2:AttributeStatement>` elements in the `<saml2p:Response>` message to be limited to one. In turn, Service Provider implementations MAY limit support to a single instance of those elements when processing `<saml2p:Response>` messages."

4.5.2 Applicability of the standard

From the vision of authorisation, the Kantara Initiative's standard doesn't improve or require much compared to the plain OASIS standard. It merely doesn't mention authorisation. However, if the authorisation would be implemented as an attribute, as suggested in 4.3.2, such practice would be compliant with Kantara's recommendations.

5 Analysis of Reference Projects

5.1 Introduction

This chapter describes the analysis of the relevant environment related to reference projects. These reference projects encompass European initiatives for the implementation of a common cross-border eID platform. Some of these eID solutions are or have been fully operational. Others are partially operational and will be fully operational within a short time-frame.

5.2 STORK 2.0

5.2.1 General information

Between 2008 and 2011, STORK has established a European eID interoperability platform, which allows citizens from one Member State to access eGovernment portals in another Member State, using their own national credentials. In STORK 14 Member States participated allowing such access with over 110 types of credentials to over 80 eGovernment portals. Most of these portals and credentials are kept operational including their cross-border interoperability.

STORK 2.0 has extended the STORK platform with legal persons, and, as a consequence, their representation by natural persons and the powers of representation. Additionally, it opened the access to the platform to the private sector as eID consumers, firstly, banks. Subsequently, it also included a great number of new, domain-specific data items, especially role-information, in order to allow (or deny) access to parts of applications. In STORK 2.0 (2012-2015) 19 Member States participated, extending the number of STORK portals with 40 new portals.

STORK 2.0 also improved the signature functionality of STORK, supporting the formats established with the Decision. In order to facilitate this support, modules from STORK, PEPPOL and especially SD-DSS solution from the EC have been combined to achieve easiest integration in applications, and the friendliest user-interface.

STORK has been used by the SPOCS project, and in STORK 2.0, pilot 4 has integrated STORK 2.0 with the epSOS NCP, as described in section 6.7.

Both the STORK and STORK 2.0 projects have ended, but the common specifications and code base are maintained by e-SENS, which supports the migration of the STORK platform to eIDAS.

5.2.2 Global view

The diagram below presents a global view of the solution:

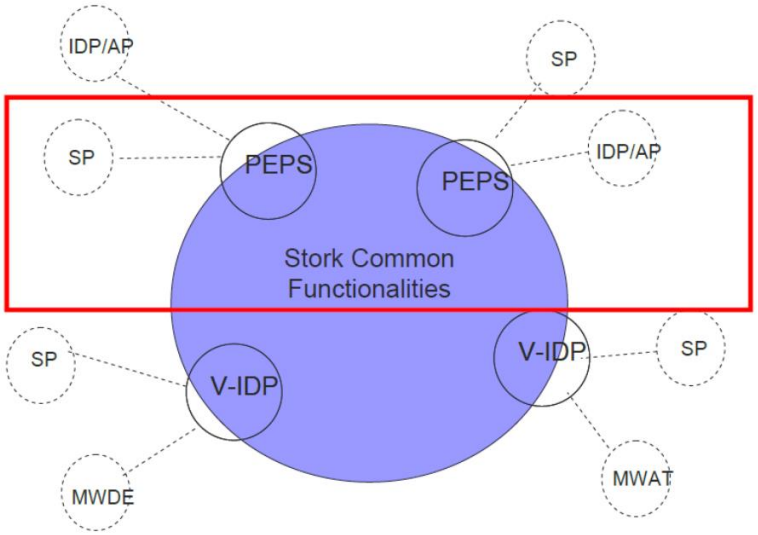


Figure 6: Nodes composing the STORK platform

The STORK solution supports federated authentication by means of an electronic ID. The messaging standard used between the STORK components in each Member State is SAML 2.0.

When a citizen asks for a service in a different country (MS A) other than from his/her native country (MS B), an authentication request is first sent by the service provider to the STORK node in this country. Next, an authentication request is transferred from the Pan-European Proxy Server (PEPS) of MS A to STORK PEPS gateway of the requested country (MS B). Once the user has identified himself to his national IDP and has given his consent to the transfer of attributes (stored by the AP) to the Service Provider in MS A, the PEPS of MS B produces an assertion containing the provided identity attributes of the user, signs it (thus vouching for its authenticity) and transmits it to the PEPS of MS A.

In the decentralised approach, a V-IDP at the Service Provider takes over the role of both PEPSs.

5.2.3 EU environment

5.2.3.1 Legal

The following directives apply and were integrated in the project [23] accordingly:

- Directive 1995/46/EC on the protection of personal data.
- Directive 1999/93/EC on a community framework for electronic signatures.

The STORK project timeline was prior to the eIDAS Regulation.

5.2.3.2 EU projects as building blocks

The STORK project, as well as the STORK 2.0 project, were EC co-funded projects under the CIP initiative. The STORK outcomes have been used in SPOCS.

With regards to other EC projects, the following building blocks have been used:

- The SD-DSS signature modules were integrated in STORK 2.0, in order to produce signatures on mainly pdf documents and XML messages (PAdES and XAdES). Also arbitrary contents are allowed (CAdES), although not piloted.
- The epSOS national contact points were integrated in pilot 4. See also section 6.7.

5.2.4 Interoperability

STORK has established an eID interoperability layer, proven in six pilots, extensible to any eGovernment application. The STORK principles and architecture have been adopted by the eIDAS regulation. STORK 2.0 has extended this layer with legal persons and their representation, which was tested in four pilots.

5.2.5 Outcome

Out of STORK came a discussion between the Member States about the legal framework for acceptance of foreign credentials: what was done during the project on a voluntary basis should be regulated legally to make such acceptance mandatory. This discussion has led to the eIDAS Regulation.

STORK 2.0 has proven that the STORK eID platform is largely extensible. However, the governance of non-core identity attributes should be organised. See also 5.2.9.4.

The STORK 2.0 platform is still operational, and all pilot portals too.

The STORK 2.0 software, together with its manuals, is published at the JoinUp portal. However, it is not considered probable that new Member States will join the STORK platform, as the CEF/eIDAS platform offers the legal support for acceptance of foreign credentials in national eGovernment portals.

5.2.6 Protocol standard

After an exhaustive study of possible standards for interchange of identity information, STORK chose SAML 2.0 as the standard for this objective. The SAML responses contain only one assertion in the case of STORK, and may contain several assertions in the case of STORK 2.0. The first assertion may be unsigned while all others are signed by the provider of these attributes. These signature provide trust and integrity. Each assertion contains at least one AttributeStatement. No other types of statements are used.

5.2.7 Available attributes

5.2.7.1 STORK Available attributes

STORK defines the following data-items in its functional design [24].

Field	*Type*	*Values and comments*
eIdentifier	String	NC/NC/xxxxxxxxxx…. (NC=NationalityCode, the first one the country of origin of the eIdentifier, the second one the destination country)
givenName	String	givenName
surname	String	inheritedFamilyName / adoptedFamilyName
inheritedFamilyName	String	inheritedFamilyName
adoptedFamilyName	String	adoptedFamilyName
gender	String(1)	F (Female) / M (Male)
nationalityCode	String(2)	ISO 3166-1 alpha-2
maritalStatus	String(1)	S (Single) / M (Married) / P (Separated) D (Divorced) / W (Widowed)
dateOfBirth	Date(basic format of ISO 8601)	YYYYMMDD / YYYYMM / YYYY
countryCodeOfBirth	String(4)	ISO 3166-3. Please note that this code is equal to ISO3166-1 alpha-2 in the majority of countries, but includes 4 letter abbreviations for disappeared countries. E.g. DDDE for the DDR or YGCS for Yugoslavia.
age	Number	In years (0..130)
isAgeOver	Boolean	Logically this is Boolean, in technical design another domain may be chosen
textResidenceAddress	Text	
canonicalResidenceAddress	XML	
residencePermit	String	
eMail	String	RFC 822

title	Text	
pseudonym	String	
signedDoc		
citizenQAAlevel	Number	[1,2,3,4]
fiscalNumber	String	

In its interface specifications [25], section 6.3 specifies the extensibility of this dataset: "Unknown attributes (attributes not listed in the […] table) in a request are ignored."

STORK 2.0 extends these data with new data items in the following categories.

5.2.7.2 STORK 2.0 new personal data

The first category is **new personal data**, with the following data item:

Field	***Type***	***Values and comments***
placeOfBirth	String	placeOfBirth is the municipality where a person was born, in national language. E.g. Firenze is not translated to Florence. Its value may change in time: Istanbul, Byzantium and Constantinople are different names for the same town.

5.2.7.3 STORK 2.0 Academic data

The second category is **Academic data**, with the following data items:

Field	***Type***	***Values and comments***
Diploma supplement	XML	
Current study supplement	XML	
yearOfStudy	Integer	1..12
averageGradeOfStudy	Decimal	
isEligibleForInternship	Boolean	

isStudent	XML	
isAcademicStaff	XML	
isTeacherOf	XML	
isCourseCoordinator	String	
isAdminStaff	String	
habilitation	String	
acTitle	enumerated	
hasDegree	XML	

5.2.7.4 STORK 2.0 Health care data

The third category is **healthcare data**, with the following data item:

Field	***Type***	***Values and comments***
isHealthCareProfessional	XML	The type of health care professional

5.2.7.5 STORK 2.0 legal person's data

The fourth category is **legal person's data**, with the following data items:

Field	***Type***	***Values and comments***
eLPIdentifier	String	NC/xxxxxxxxxxxx... (NC = Nationality Code, the country of the organisation, xxxxx is the national identifier, usually the VAT number or the inscription number at the Business Register of the legal person)
legalName	String	Official name of the legal person
alternativeName	String	Commercial name of the legal person
type	String	

translatableType	enumerated	
status	enumerated	
activity	enumerated	
registeredAddress	String	
registeredCanonicalAddress	XML	
contactInformation	String	Name, Email and/or phone number
LPFiscalNumber	String	

5.2.7.6 STORK 2.0 mandate

The fifth category is the **mandate** with just one attribute:

Field	***Type***	***Values and comments***
mandate	XML	

5.2.8 Discussion on the mandate

It is evident that a legal person cannot take decisions, enter into a contract, sign a document etc., except through a natural person who represents that legal person and acts on its behalf. This power is given through a mandate.

5.2.8.1 Legal aspects of the mandate

STORK 2.0 exhaustively studied the legal requirements of mandates, of which the conclusions are reflected in "D3.6 Consolidated Legal Entities Report" [26]. Chapter 2 of that document explains the following points about mandates.

5.2.8.1.1 Mandates *ex lege* within legal entities

The basic rule accepted in all participating countries is that the charter and/or the act of incorporation of the legal entity establish who has the mandate to manage and represent the legal person. With 'act of incorporation', we mean the document (usually, but not necessarily and not always, a deed) through which the founders created the legal entity, while 'charter' indicates the document where the basic working rules of the legal entity are set forth.

Given that the directors of the legal entity have the mandate to represent the company, this mandate must be granted in the charter or in the act of incorporation, or, in several participating countries, by the general assembly of the legal person in an ad hoc document (voted and approved by the general assembly).

This mandate cannot be freely derived from external circumstances (e.g. behaviour of a natural person) and requires an explicit reference in the charter or act of incorporation, and reflection in a business register. Thus, the main challenge is to identify a reliable source of this information at the national level, and ensuring that the resulting information can be used in a trustworthy manner.

5.2.8.1.2 Mandates and daily administration of legal entities

All jurisdictions in STORK 2.0 allow mandates for daily administration, although there are some small divergences in how this is done. Generally, such a mandate will be given by virtue of a decision of the general assembly of the legal person or, in some countries, in the act of incorporation or charter as well, or finally in an ad hoc contract between the legal person and the daily manager. The mandate can be given to a director of the legal entity, to an employee or to a third party; such a mandate is generally published in the commercial register. This means that these countries should have reliable databases of mandates for legal entities which may be useful for STORK (depending on their accessibility). […]

5.2.8.1.3 Chained mandates

Although only natural persons have the ultimate capacity to take decisions, to vote, to think about strategies etc., legal persons can also be chosen as directors (and thus have a mandate to represent and manage the legal entity) of another legal person. This leads to an embedded structure (a 'chained mandate', where a legal person is represented by another legal person, etc., until ultimately a natural person is found in the chain to express the actual decisions). Thus, chained use cases need to be supported where multiple chained mandates need to be resolved, without degrading the trustworthiness of the validation process.

The simplest case of a chained mandate is when the (authenticated) end-user's powers derive from a mandate to represent another person who is the official representative of the company. By way of example, an accountant logs in to a website via STORK 2.0. The accountant has received a mandate from his client to file taxes on behalf of company X, of which the client is general manager and legal representative. In this case, the service provider may need to establish the continued validity of both the end-user's mandate (i.e. the accountant's mandate to file taxes on behalf of the company) and of the powers of the mandating person (i.e. the client's continued competence to grant this mandate to the accountant). This second step involves the verification of powers of a person, the client, who is not currently in session, but whose delegated agent, the accountant, is.

5.2.8.2 Sub-attributes of the mandate

As this attribute is very relevant for this document, this study includes more details about it. The subordinate attributes of the mandate are:

Name	***Type***	***Description***
Representative	XML	
Represented	XML	

MandateContent	XML	• *timeRestriction*
		  ○ *validFrom*: the date from which the authorisations are valid (date)
		  ○ *validTo*: the date up to which the authorisations are valid (date)
		• *transactionLimitRestriction*
		  ○ *amount*: the maximum amount of money that the representative may commit in a financial transaction (number)
		  ○ *currency*: the currency of the amount (String)
		• *isJoint:* Indicates whether or not the power is joint with other persons, and if so with whom, in a semicolon separated list
		• *isChained:* indicated whether or not the mandate is chained. However, in the reply to the Service Provider the represented person is the principal and the representative is the user in session.
		• *originalMandate: The original text of the mandate in original language*
		• *originalMandateType: the type of data included in the originalMandate. Possible values: text/plain, image/jpg, image/gif*
		• *AQAA: the quality of these data, integer [1 .. 4]*
		• *typeOfPower*: limitation of the mandate to the following types of powers
		  • **General powers**: […]
		  • **Commercial powers** […]
		  • **Human Resources powers** […]
		  • **General services powers** […]
		  • **Financial powers** […]

		• **Public interest representation powers** […] • **Health powers** […] • **Other powers** […]

The first two attributes indicate legal or natural persons who have mandated the other person to perform certain actions on behalf of the first person. Several mandates can be chained, as well in one assertion with a multiple-valued mandate (from one country's register) or in several assertions (from different, possibly cross-border registers).

5.2.9 Governance

5.2.9.1 Governance process

The STORK specifications and code are currently maintained by the e-SENS project, which has this governance organised at work package level. The long term governance of STORK is not established. Major decisions are taken by their General Assembly.

5.2.9.2 STORK 2.0 parameter governance

Most Member States will maintain their STORK infrastructure for a few years. This means that any change in the parameters, especially renewal of certificates is partially performed by the version control function. This function publishes a tailor-made XML file with the main characteristics of the national system, which is downloaded by other STORK nodes. If any change is detected in a foreign VC file, as far as required, the corresponding parameter in the national node is adapted, and in addition, a mail is sent to the systems administrator in order to perform some interoperability tests.

For those MS which don't have the version control function installed, this is complemented with direct communication by email between the affected MS, after which changes are applied manually.

5.2.9.3 STORK 2.0 common specifications and code maintenance

Both the STORK project and the STORK 2.0 project have ended. Currently e-SENS maintains the common specifications and code base. However, in the future, when the e-SENS project ends, no continuation of the maintenance is foreseen.

5.2.9.4 STORK 2.0 data governance

The STORK project team foresaw that the definition of the complete set of attributes should not be the responsibility of the MS. For "domain-specific" attributes this responsibility should reside in domain-specific organisations. eIDAS encompasses a similar approach, focusing on the mandatory minimum data-set and allowing for a sector specific part where domain specific attributes could be exchanged seamlessly.

So, in STORK 2.0's Functional Design, section 2.3, the project team stated the following concerning the "domain specific" attributes [24]: "The domain-specific attributes, detailed in the following sections, form a series of innumerable data items which describe a person from different (business or domain specific) points of view. STORK 2.0 designed a flexible infrastructure allowing each type of domain to define their attributes, without the central infrastructure interfering."

Currently, the "core" attributes are maintained by the e-SENS organisation, which is responsible of the STORK maintenance until at least eIDAS becomes mandatory for the MS.

According to the technical specifications of STORK 2.0 [27], "if any unknown attribute is requested, it will be ignored. Nevertheless, if such unknown attribute is marked as mandatory the request is rejected". Hence, in practice, technically speaking, if a domain specific attribute is mandatory for the Service Provider, it requires that all MS implement the new custom attribute regardless of if they need it or not, or alternatively, the user will receive an error-page at these MS.

5.3 CEF/eID

5.3.1 General information

Based on the eIDAS regulation, expert groups have agreed on the eIDAS specifications [28], which have been implemented in common building blocks by DIGIT under the CEF program. Currently, several MS are deploying their eIDAS node, but, at the time of writing, no national issued eIDs have been notified so far.

5.3.2 Global view

The diagram below presents a global view of the solution:

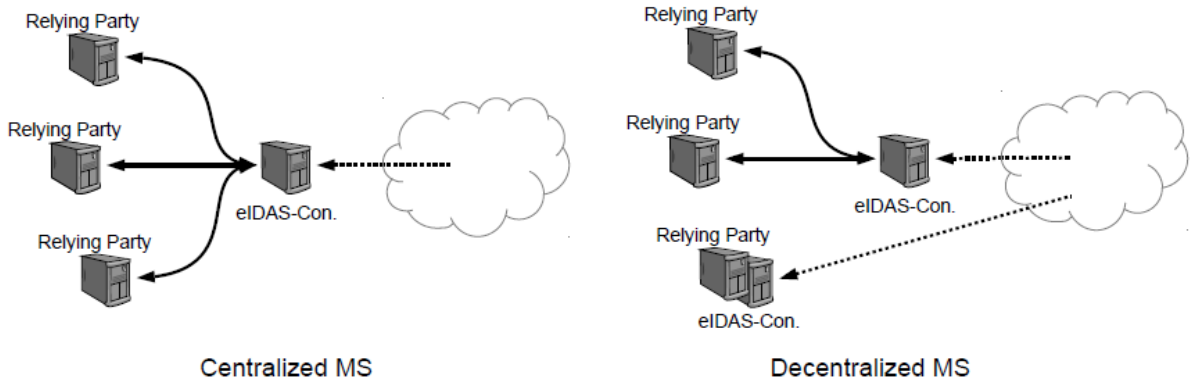


Figure 7: eIDAS architecture with centralised and decentralised nodes

In fact, this architecture is similar to the one used for STORK. An eIDAS connector (like the S-PEPS) is located in each country with a centralised architecture serving foreign eIDs to its national relying parties.

Such connector is decentralised in other countries: some have a connector for each relying party while others may use one eIDAS connector serving several relying parties.

In addition, eIDAS nodes also exist for serving nationally issued eIDs: one eIDAS server is located in each centralised MS for its own credentials, and decentralised eIDAS servers for decentralised countries are located in all other MS.

5.3.3 EU environment

5.3.3.1 Legal

The following directives apply and were integrated in the project [23] accordingly:

- The eIDAS regulation [3], its implementing acts and technical specifications.
- Directive 1995/46/EC on the protection of personal data.
- Directive 1999/93/EC on a community framework for electronic signatures.

5.3.3.2 EU projects as building blocks

The CEF/eIDAS specifications, reference code, etc. form the eID building block. This building block has the long term governance organised and also legal support, the Regulation, which obliges all MS to adopt this building block before September 2018.

5.3.4 Interoperability

The CEF/eIDAS building block is the new eID interoperability framework, as defined by the eIDAS regulation.

5.3.5 Outcome

At the time of writing, the CEF/eIDAS building block is being deployed by several MS. However, currently, no nationally issued eIDs have been notified to the Commission. All MS will deploy this building block before September 2018.

5.3.6 Protocol standard

The eIDAS technical specifications have established SAML 2.0 as the standard for the exchange of identity information. The SAML responses contain one assertion, with at least one AuthnStatement, and optionally one or more AttributeStatement-s.

The CEF/eIDAS attributes are adopted from the SEMIC Core Person Vocabulary and Core Business Vocabulary.

5.3.7 Available attributes

5.3.7.1 eIDAS mandatory attributes for natural persons

eIDAS defines [8] the following data items in its specifications.

Field	***Type***	***Values and comments***
FamilyName	String	Current Family Name
FirstName	String	Current First Names
DateOfBirth	String	Date of Birth
PersonIdentifier	String	Uniqueness Identifier

In its interoperability architecture [29], section 1.3 specifies the extensibility (robustness) of this dataset: "Implementations should follow a general principle of robustness: be conservative in what you do, be liberal in what you accept from others."

5.3.7.2 eIDAS optional attributes for natural persons

eIDAS extends the previous dataset with optional data items.

Field	***Type***	***Values and comments***
BirthName	string	First Names at Birth
BirthName	string	Family Name at Birth
PlaceOfBirth	string	Place of Birth
CurrentAddress	multiple string elements	Current Address
Gender	selection: Male, Female, Not Specified	Gender

5.3.7.3 eIDAS legal person's mandatory data

Field	***Type***	***Values and comments***
LegalName	string	Current Legal Name
LegalPersonIdentifier	string	Unique Identifier

5.3.7.4 eIDAS legal person's optional data

Field	Type	Values and comments
LegalAddress	Multiple Strings	Current Address
VATRegistration	String	VAT Registration Number
TaxReference	String	Tax Reference Number
BusinessCodes	String	Directive 2012/17/EU Identifier
LEI	String	Legal Entity Identifier (LEI)
EORI	String	Economic Operator Registration and Identification (EORI)
SEED	String	System for Exchange of Excise Data (SEED)
SIC	String	Standard Industrial Classification (SIC)

5.3.8 Governance

5.3.8.1 Governance process

The eIDAS expert group expects the requests of domain specific groups to verify the eIDAS compatibility and overall coherence of their inquiries. At the time of writing, an eIDAS governance process of such domain requests is not yet in place. However, it could be envisaged that includes some activities as follows:

- Domain specific attributes should be proposed to the technical eIDAS technical sub-group for consideration.
- If accepted, the eIDAS technical sub-group will help in the identification of domain experts that will work for the attribute schema specification.
- The eIDAS technical sub-group experts could provide advice regarding attribute schema design on request.
- The eIDAS technical sub-group would provide a final review of the completed specification.
- The agreed domain specific attribute schema should be published alongside the core eIDAS specifications on the CEF portal.

When the first domain specific expert group will be established, also the collaboration and communication process will be defined.

5.3.8.2 eIDAS data governance

No changes in the available data (minimum dataset and optional data) in the specifications are yet foreseen.

The foreseen changes are to be part of the domain-specific data, to be defined and maintained by domain experts, with the eIDAS Technical Sub-group playing a “sense checking” role prior to publication of each attribute schema. This would ensure that duplication across domain specific attribute sets is minimised and that the encoding of data is as consistent as possible across the federation.

At the time of writing, no domain expert group has been established. Such group should define its governance organisation, processes, etc. When establishing the first domain expert group, the collaboration process and communication should be defined.

5.4 e-SENS/eID

5.4.1 General information

e-SENS (Electronic Simple European Networked Services) is a large-scale project that embodies the idea of European Digital Market through innovative ICT solutions. It faces technical and legal challenges by providing solutions for seamless public service delivery across borders. e-SENS consolidates, improves and extends existing technical solutions to develop a coherent and sustainable European Interoperability Architecture.

e-SENS covers different aspects of ICT applied in a number of cross-border cases in domains such as e-Health, e-Justice, e-Procurement and business setup. The e-SENS solutions based on standards and technical specifications can be combined with each other and integrated with sector-specific applications. The goal of generic and reusable components is to enable any information systems to offer services across national borders and sectors to businesses and citizen.

e-SENS embodies several modules, extending and integrating earlier projects, like eHealth (epSOS), eProcurement (PEPPOL), eJustice (e-CODEX) and eGovernment (SPOCS), as well as cross-sector generic modules like eID (STORK), eDelivery, eSignatures and eDocuments. These services are piloted in several national portals. The relevant module for this study is the eID module.

Since the start of 2016 e-SENS has taken up the maintenance of the eID modules delivered by the STORK 2.0 project.

5.4.2 Global view

The diagram below presents a global view of the solution:

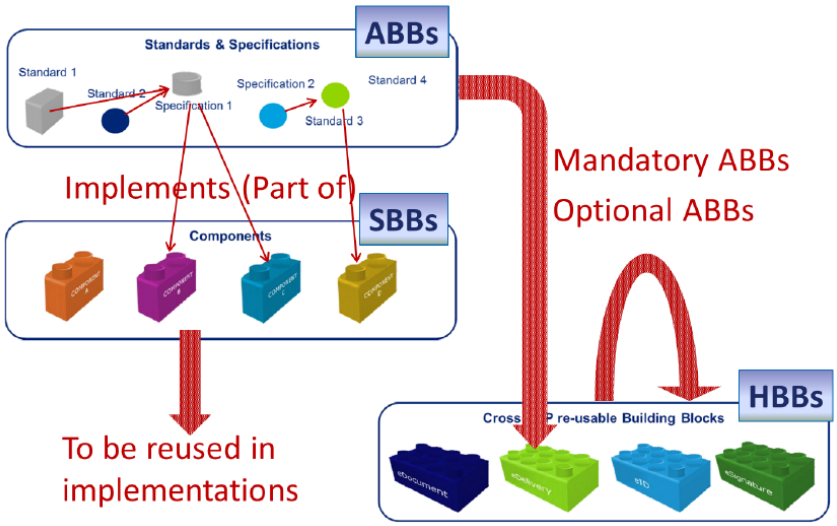


Figure 8: e-SENS abstract building blocks and their relationships

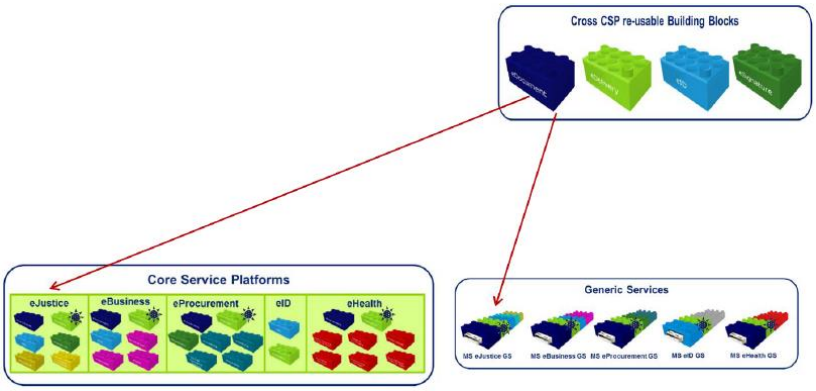


Figure 9: e-SENS building blocks and their usage

Note: Only the eID building block is relevant for this study.

5.4.3 EU environment

5.4.3.1 Legal

e-SENS builds upon the legal requirements and findings from other projects, as described in 5.2.3.1 for STORK, 5.3.3.1 for eIDAS-CEF, 6.2.3.1 for epSOS, 6.4.3.1 for eCODEX and 6.3.3.1 for SPOCS.

5.4.3.2 EU projects as building blocks

e-SENS embodies several building blocks, extending and integrating the results from earlier projects, like eHealth (epSOS), eProcurement (PEPPOL), eJustice (e-CODEX) and eGovernment (SPOCS), as well as cross-sector generic modules like eID (STORK), eDelivery, eSignatures and eDocuments.

Furthermore, since the start of 2016, e-SENS has taken up the maintenance of the eID modules delivered by the STORK 2.0 project.

Those services are piloted in several national portals. Of these building blocks not only the technical infrastructure is used, but also the governance is studied in order to propose an enduring governance solution for each module.

5.4.4 Interoperability

e-SENS maintains the interoperability of the common solutions for eID, eDelivery, eSignature, eDocument, etc. e-SENS also maintains the interoperability of eHealth, eProcurement, eJustice and eGovernment solutions. This maintenance includes the agreement of required changes in the specifications, its development and test, and finally the implementation of the changes.

5.4.5 Outcome

The e-SENS project is still alive, so the outcome may still change. For the moment, its most important contribution to sustainable European solutions is its studies and proposals on governance.

5.4.6 Protocol standard

As far as eID is concerned, e-SENS has adopted the STORK / STORK 2.0 and eIDAS specifications. Furthermore, e-SENS is smoothing the migration path for the eID building block from STORK to eIDAS.

5.4.7 Available attributes

e-SENS maintains the STORK 2.0 attribute collection.

5.4.8 Governance

e-SENS has performed several studies on the needs for governance in each of its aspects, and evaluated by each of the MS [30]. In 2014, it also studied the possible governance solutions foreseen for each of the building blocks [31]. As far as eID is concerned, this last report could not anticipate the present situation, and hence doesn't present a concrete solution for STORK after e-SENS.

5.5 Previous Phase of ISA Action 1.18

The analysis of the Previous Phase of ISA Action 1.18 is also included in the Reference Projects chapter. Unlike the other reference projects, it extends the cross-border eID platform, which is based on the ECAS-STORK integration, to **demonstrate the feasibility of a federated authorisation solution** on top of such integration. The Previous Phase comprised of the following activities: requirements gathering, architecture specification and proof-of-concept.

As this previous phase was just a proof-of-concept, it isn't operational anymore. As a consequence, the solution for federated authorisation proposed in this document doesn't need to fit in the resulting platform. However, the results of this phase have many aspects similar to the reference projects; this is the reason for including this initiative in the current chapter.

5.5.1 General information

The Previous Phase of ISA Action 1.18 was conducted between 2013 and 2014. The aim of the project was threefold:

- Collect a set of **needs and requirements** from stakeholders in order to shape the capabilities of the federated authorisation solution. The stakeholders that participated were: MSs, STORK representatives, ECAS representatives, EC Application owner (only from the CircABC EC application).
- **Design** the necessary transformation of the ECAS and STORK components that should support the federated authorisation solution.
- Implement a **proof-of-concept** to test the feasibility of architecture decisions that were defined for such federated authorisation solution. In order to demonstrate all the possible scenarios, the pilot comprised of real components (such as CIRCABC as EC application, STORK non-PEPS (V-IDP) from Austria MS) and also mock-up components (STORK PEPS mock-up).

5.5.2 Global view

The diagram below presents a global view of the solution:

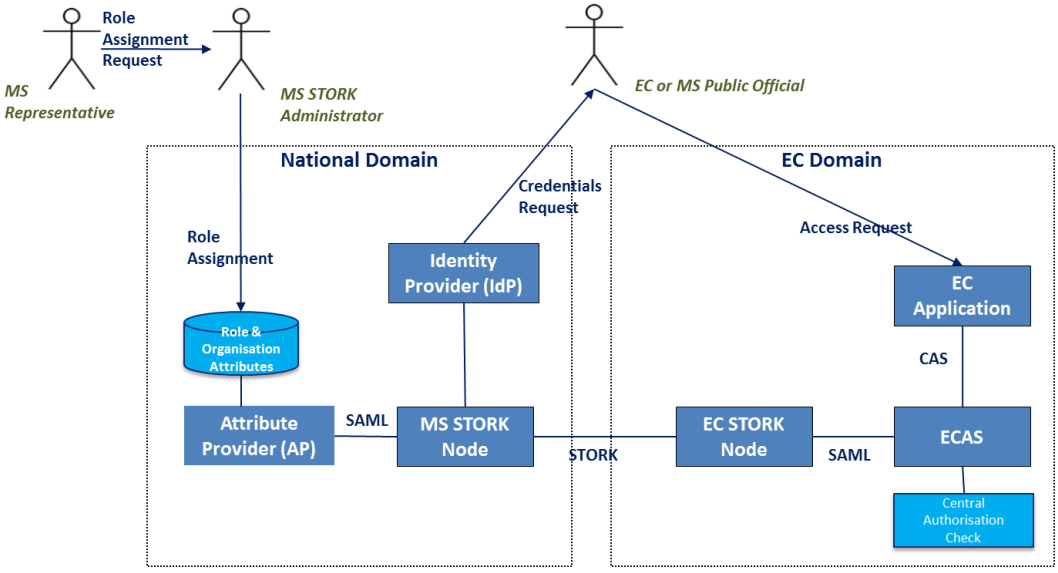


Figure 10: Previous Phase of ISA Action 1.18 systems' domains view

The proposed solution was driven by the following architecture decisions:

- **Authorisation was based on the information received from the MS, via STORK, about the user role** in the context of the EC application. On the basis of this additional user information received (role and organisation attributes), an authorisation can be done in the application at any time, in order to decide if the user has granted access to the requested EC application or service.
- Two **additional SAML attributes** were included to the STORK request and response messages. These attributes were: **organisation** and **role** of the user in the context of the EC application. The agreed usages for the attributes were:
    - The roles transmitted were EC application roles, which were not MS specific. The roles carried out information not only about the role itself but also about the EC Application to which it is related. The format of the attribute was as follows: AppName/RoleName.
    - Organisation was the reference attribute to implement an additional check of the validity of the roles. This check was done at a central level in the ECAS infrastructure.
- ECAS did not perform any check on whether an organisation was allowed to assign a specific role to one of its users. **ECAS trusted the validity of the attributes received via STORK**. ECAS requested these attributes to the STORK component and they were returned to ECAS upon successful STORK authentication.
- **MS did the mapping of roles** between the user's internal roles within the organisation and the EC Application roles.

The global authorisation process designed is shown below:

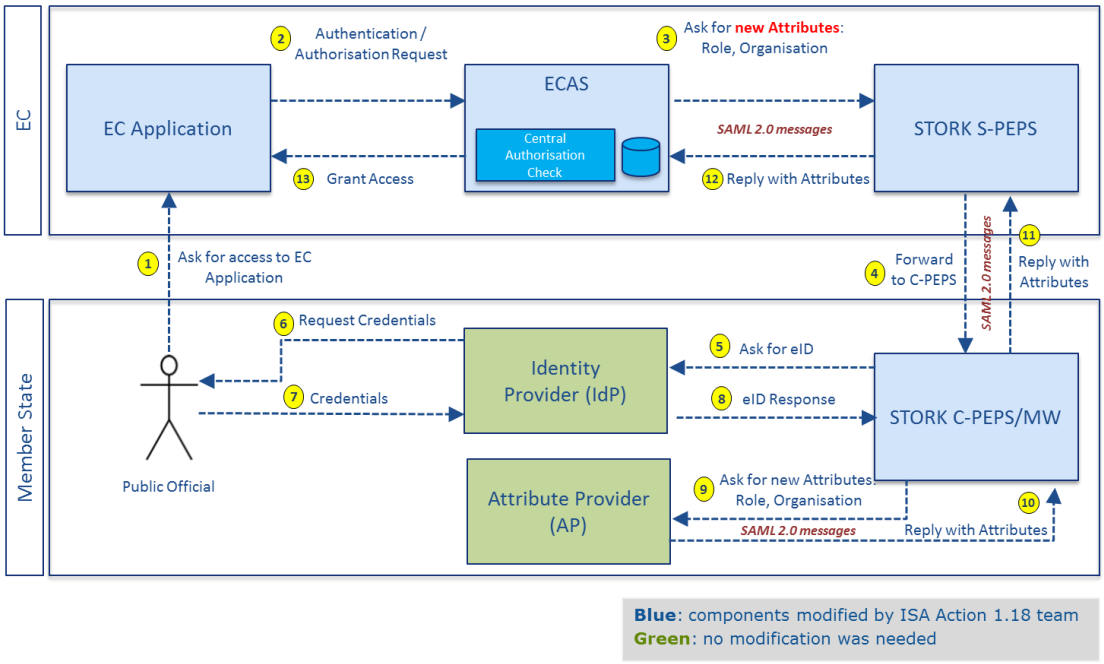


Figure 11: Previous phase of ISA 1.18 – Global authorisation process

The overall process sequence is as follows:

- When any user tries to access a protected resource, the ECAS client validates if he is logged in.

- If the user is not logged in, the user gets redirected to ECAS server authentication portal.
- Then, a country selection page will be presented and the user will pick the country where he wants to authenticate.
- The SAML request constructed by the ECAS server is sent in this request along with the selected country to the S-PEPS (or Service Provider PEPS) which is the PEPS component deployed in the EC domain. After validation of the selected country, a request is sent to C-PEPS in the citizen's MS (or Citizen PEPS).
- After sending the consent form with the SAML request to the C-PEPS the user is redirected to the IDP of the selected country where a login form allows the authentication. Upon successful authentication, the IDP will send the response to the C-PEPS and the user will then be redirected according to that response to the corresponding AP.
- The user request to the AP results in a set of values for the attributes selected, and following that step, a redirection to the C-PEPS takes place for a final validation, where the user gets a consent page with the attribute values that are about to be transferred to the ECAS domain. The response obtained includes the SAML response for the S-PEPS. Finally, the request is sent to the S-PEPS, and after that the user gets redirected back to ECAS server.
- The message sent to ECAS server after STORK authentication is the SAML response. With that information, the ECAS server processes the response and builds the corresponding reply to the application using the values received from STORK.
- ECAS client, before allowing the user to access the application, validates the received information with ECAS server. Here is where the ECApplicationRole attribute received from STORK is processed. At this point, the ECAS server performs a central authorisation check, verifying if the list of roles received are valid for the provided MS organisation.
- The response sent back to ECAS client after validation success contains, amongst other things, a list of roles. From that moment they are available to the EC application so they can be retrieved for use for authorisation purposes.

5.5.3 EU environment

5.5.3.1 Legal

The solution complied with national and EU level regulations, in particular, concerning the transmission of personal information at the time of project execution (2013-2014).

5.5.3.2 EU projects as building blocks

The Previous Phase of ISA Action 1.18 re-used the ECAS-STORK integration. Such integration was already on place at the time of project execution.

5.5.4 Interoperability

The Previous Phase of ISA Action 1.18 kept the same level of interoperability as the one provided by STORK because it was based on STORK and no change was introduced in the specification nor in the protocol message format.

5.5.5 Outcome

The Previous Phase of ISA Action 1.18 successfully demonstrated the following:

- ECAS-STORK integration can be extended to exchange new SAML attributes with role information intended to support an authorisation process.

5.5.6 Protocol standard

The Previous Phase of ISA Action 1.18 adopted the STORK protocol standard.

5.5.7 Available attributes

The Previous Phase of ISA Action 1.18 maintained the STORK attribute collection, but added the following custom attributes:

- **Role**. This role referred to specific roles of the EC application, which were different from the ones from MS. The roles carried information not only about the role itself but also about the EC Application to which it is related. The format of the attribute was as follows: AppName/RoleName. This attribute was used in the EC application to verify at runtime if the user had granted access to certain services/features of the application.
- **Organization.** This attribute carried out information about the organisation which the user belongs to. This attribute was used to implement an additional check of the validity of the roles. This check was done at a central level in the ECAS infrastructure.

5.5.8 Governance

When new roles were created in the EC application used for this demo (e.g. CIRCABC), the ECAS team communicated the newly created roles to the Member States participating in the pilot. Such communication was in off-line mode because no automated procedure was agreed upon.

Also, the introduction of the new attributes in the STORK infrastructure was done without following any governance procedure.

5.6 Findings

From the reference projects the following findings have been extracted:

Description	Field of influence	Source
Universal participation. MS participation was crucial for the sustainability of the cross-border eID solutions. Participation of all 28 MS, plus the participants of the EEA was only achieved in eIDAS.	Governance	All
Extensibility. eID solutions should be extensible with new attributes, without breaking the interoperability.	eID solution	All
Incomplete standardisation. Many parallel developments have caused a lack of synchronisation. E.g. as SEMIC was started after STORK, STORK couldn't adopt their names.	eID solution	All
Sovereignty. Solutions must be respectful of MS sovereignty, and not **interfere** with national infrastructure.	Governance, eID solution	All
Usage of **SEMIC Core Vocabularies.** eIDAS is the only reference project that uses some SEMIC Core Vocabulary. More specifically, Person and Business Core Vocabularies were reused in the project.	eID solutions	eIDAS
Cross-border attributes. STORK 2.0 allows cross-border collection of one person's attributes, including mandates.	Cross-border eID solution	STORK
Domain specific attributes implementation. Technically speaking, if a domain specific attribute is mandatory for the Service Provider, it requires that all MS implement the new custom attribute regardless of if they need it or not, or alternatively, the user will receive an error-page at these MS. Also, e-SENS reported that handling new custom attributes was too heavy concerning governance and implementation.	eID solution	STORK

Table 2. Reference Projects - Major findings

6 Analysis of Domain Specific Projects

6.1 Introduction

This chapter summarises the analysis of the relevant environment related to domain specific projects. These projects are focused on domain specific challenges but all have to face cross-border authentication and authorisation.

It should be noted that only one project, the UUM&DS, is intended to be a production-ready system. The other projects analysed are LSP that developed practical solutions tested in real government service cases across Europe in three different areas: eHealth (epSOS and STORK 2.0 Pilot 4), eJustice (e-CODEX), and eBusiness (SPOCS and STORK 2.0 Pilot 3).

The **topics analysed** for each project are the following:

- global view of the solution,
- EU environment and synergies with other projects,
- authentication and authorisation processes,
- interoperability,
- governance approach, and
- outcome.

This information is synthesised in section 6.8 as findings that will **influence** recommendations and experience for the potential solution.

6.2 epSOS (European Patients Smart Open Services)

6.2.1 General information

epSOS [32] is an eHealth interoperability project co-funded by the EC. It aims at improving medical treatment of citizens while abroad by providing the Health Care Professional (HCP) with the necessary electronic and safe patient data. The goal of the project is to develop a service infrastructure that enables the exchange of patient data across borders in order to offer seamless healthcare to citizens. This improves the quality and safety of healthcare for citizens when travelling. This is relevant for tourists, business travellers, exchange students or regular cross-border commuters experiencing unexpected health problems. This cross-border exchange is subject to the patient's consent.

To this end, a service infrastructure was designed, built and evaluated to demonstrate the secure cross-border interoperability. The project developed technical, legal and organisational concepts towards these objectives.

At the time of writing, epSOS has ended. The project was initiated in July 2008 and came to an end in June 2014.

25 different European countries were involved: 22 EU Member States and 3 non-EU Member States.

6.2.2 Global view

The diagram below presents a global view of the solution:

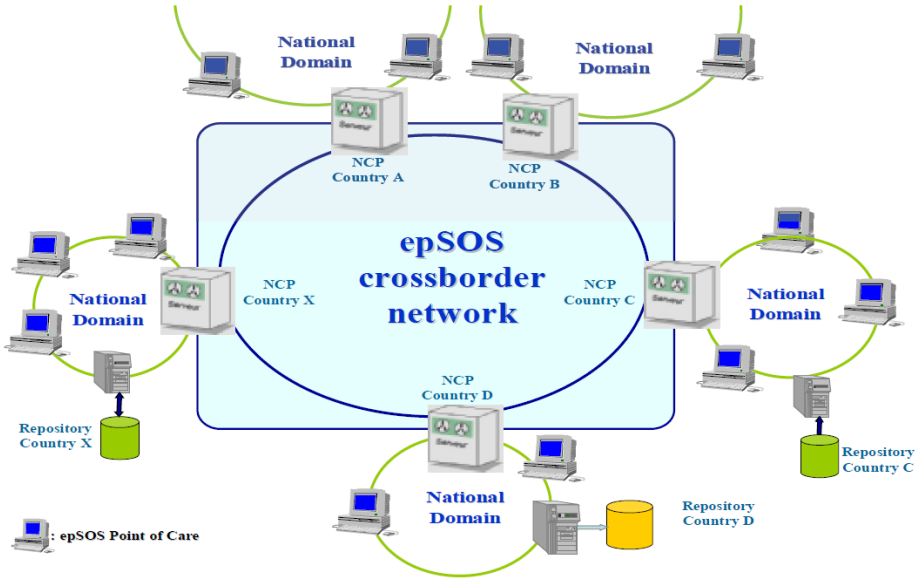


Figure 12: epSOS LSP global view topology. Source: [33]

Initially, patient health data is created, stored and processed in various systems of national (e-Health) domains apart from the epSOS environment. When a patient is abroad and inquiries his health data, he or she accesses the epSOS services. These services transfer agreed data, particularly, a patient's summary and prescriptions. Since the system deals with sensitive data, before utilising the epSOS services it is necessary that a successful identification and authentication of the HCP, the identification of the patient, and a valid role assigned to the requestor of the data are performed.

To this end, the national domains of MS are connected to the epSOS system by National Contact points (NCPs), which serve as gateways. Since all epSOS communications among HCPs from different countries run through NCPs, each NCP must be able to prove its identity and to validate the identity of its partner (another NCP), before sending the requested data. As can be seen, the NCP concept of epSOS fits perfectly with the PEPS/V-IDP component of STORK.

6.2.3 EU environment

6.2.3.1 Legal

The following directives apply and where integrated in the project [23] accordingly:

- Directive 1995/46/EC on the protection of personal data.

- Directive 1999/93/EC on a community framework for electronic signatures.
- Directive 2006/123/EC on services in the internal market.
- Directive 2005/36/EC on the recognition of professional qualifications.

Moreover, the European eHealth interoperability is supported by the Directive 2011/24/EC.

6.2.3.2 EU projects as building blocks

The project explored the following collaborations and interdependencies with other EU projects [33] in order to take advantage of reusable components and common issues.

With regard to STORK 1.0, the following synergies were identified:

- Identification and authentication of a patient, while abroad, but only when having an eID. In this case, the epSOS LSP process flows are basically the same as the STORK PEPS/V-IDP authentication flows. Even the exchanged tokens through STORK could be utilised in epSOS.
- Security levels to give better protection to sensitive parts in epSOS LSP. For example, updating data could require a different security level than reading them. The "quality assurance levels" approach of STORK could be used to apply those security levels.

Thus, the collaboration with STORK 1.0 was strongly recommended and several bi-lateral meetings were held. However, STORK 1.0 was not used on the epSOS pilots. Among the main reasons we can point out: one authentication use scenario was not supported by STORK, and the project agreement on that MS infrastructure was responsible for the authentication.

Finally, it should be mentioned that, as already described in section 6.7, STORK 2.0 rolled-out a set of domain specific pilots. eHealth was one of the domains chosen and the infrastructure of epSOS was reused to realize the integration with STORK and test some eHealth use cases.

6.2.4 Authentication

In the context of epSOS, identification was a necessary and complex capability because of the eHealth specific constraints mainly related to the patient's privacy and HCP confidential access. After an in-depth analysis of the epSOS use cases, it was concluded that the multilateral authentication and authorisation processes should be implemented in the national infrastructure. The motivations were related to functional and governance aspects [33].

To this end, epSOS LSP specified [34] technical means to transport and communicate identity information irrespective of the final MS authentication mechanism (e.g. eID based on smart-card, user/password, etc.). These technical means were based on the **WS-Security** standard. The epSOS interfaces were specified on the basis of this standard, which is independent of the approach used by the relying parties (MSs) to authenticate. Moreover, the identification and authentication processes supported different configurable configurations in order to provide compatibility with the MSs solutions and requirements.

6.2.5 Authorisation

The solution chosen concerning Authorisation was to implement an Access Control System (ACS) [34]. The objective of the access control security service is to provide a means for the MSs to enforce access controls on resources without interfering within the local legislation, at the NCP level. The definition of the MS's trusted domain was written in a policy document, in a specified formalism that an ACS can process and enforce. In epSOS, the access policy consisted of patient policies (policies that the patient defines for giving his/her privacy consent) and MS policies defined for alignment with the MS' local legislation.

This approach was coherent with the epSOS philosophy where the pilots must not require any changes to national health systems, and each MS must self-rule the policies according to the local legislation. Also, this solution can be enriched with additional attributes. This led to a more detailed approach named Attribute Based Access Control (ABAC), a superset of the RBAC that includes all the functionalities and adds the possibility of using more attributes in the access decision rather than the simple role. The evolution of the ABAC model is the Policy Based Access Control (**PBAC**) where every resource or a group of resources have a policy governing the accesses. This was the model adopted by the Access Control Security Service.

The idea was to provide an Access Control Service in front of each epSOS-NCP that intercepted all queries and enforced policies. (See Figure 13 below).

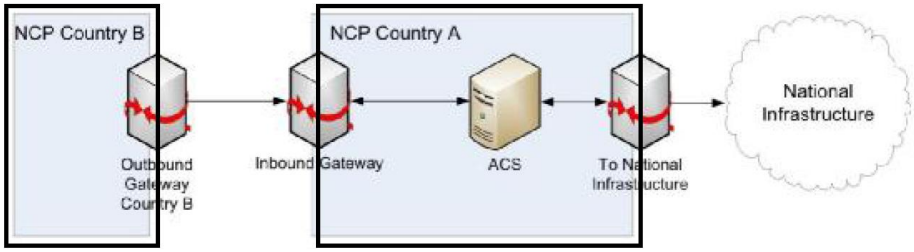


Figure 13: epSOS Access Control Service Security architecture. Source: [34]

In order to implement the solution in a standard way, the **XACML** specification was chosen [34]. XACML allows for specifying standard access control policies in a machine-readable format. A policy comprises of a set of targets (the resource to be protected) and rules (such as read/write). The XACML policy editors are free to write their own policy model. This made XACML an ideal solution for the epSOS Access Control Security Service.

In epSOS, the definition of policies was based on roles. Active actors of epSOS LSP were categorised with respect to their tasks and positions in epSOS and standardised sets of privileges were assigned to each role. A role is a special attribute that specifies a collection of privileges to access or use resources available in epSOS. After a successful authentication, the user was linked with a role (**attribute**) and thus serves as an input for the authorisation process to be enforced by the ACS. The medical roles selected for epSOS were: Medical Doctors, Nursing and Midwifery professionals, and Pharmacists.

epSOS used parts of a Policy-Based Access Control (PBAC) mechanism for the decisions which are not only based on the roles, but also on attributes (e.g. “Purpose of use”, “Locality”) and additional modified restrictions following from patient consent.

6.2.6 Interoperability

epSOS chose the European Interoperability Framework (**EIF**) for European public services [35] as the interoperability framework reference to specify the level of interoperability support of different system’s components. On the basis of EIF, epSOS defined a tailored interoperability framework. The following diagram shows the final interoperability framework layers adopted by epSOS:

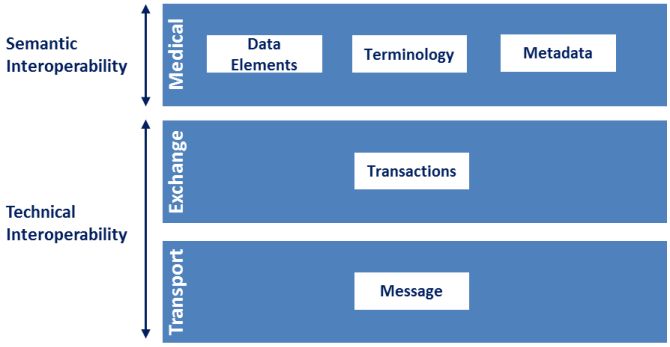


Figure 14: epSOS Interoperability framework. Source: [23]

Considering the epSOS time frame for implementation of the pilots, the existing experiences in industry and the strong demand for standardised security measures, a decision on the top-level messaging protocol was made [23] to use the **W3C SOAP** protocol.

The choice of standard for encoding the security token was the **SAML 2.0** (Security Assertion Markup Language). SAML assertions can be integrated within SOAP security headers and are compatible with WS Security and the WS* family of specifications. SAML allows for making assertions regarding the identity, attributes, and entitlements of a subject to other entities, such as a NCP or a HCPO.

The Integrating the Healthcare Enterprise (IHE) Europe organisation participated ensuring uniform **adoption of international standards through profiling**.

6.2.7 Governance

Regarding the national healthcare solutions, they can vary strongly and there was no obligation for stakeholders to use any common solution. However, some Member States decided to deploy eHealth solutions on a large scale on the basis of epSOS specifications and interoperability framework.

Currently there are two active EU initiatives, the eHealth Network and the eHealth Governance Initiative (eHGI), which are the most prominent candidates to conform to an eHealth governance body that ensures development and sustainability of the eHealth assets and solutions. These organisations also

represent the private sector, which is of crucial importance as well. This governance body should lead at EU level the federation and harmonisation of the patient data exchange to ensure interoperability.

6.2.8 Outcome

It should be noted that the eHealth sector has specific requirements that were not sufficiently met by generic building blocks.

Each Member State was fully responsible for ensuring the security, confidentiality and integrity of the technical systems and for implementing electronic identification schemes at national level. Consequently, epSOS did not specify any technical or procedural requirements to harmonise the security, confidentiality and integrity of national systems but reached agreements on adequate security and audit requirements and a common security and audit policy specific to the cross-border settings.

epSOS Member States shared, discussed and agreed on common minimum requirements and practices based on EU and international standards to ensure and enhance security [36]. Further technical eID interoperability of epSOS was developed in the FutureID project.

Finally, the epSOS results are currently taken forward by various endeavours:

- **OpenNCP** [37]. It offers a ready-to-deploy NCP eHealth solution. OpenNCP is an open community that maintains and evolves epSOS. Includes a set of eHealth components that can be used separately. Currently, the integration with the CEF/eID is in progress.
- **EXPAND** ("Expanding Health Data Interoperability Services") [38]: It maintains the epSOS pilot services and where appropriate expand them by re-using mature assets from other pilot projects, up to the launch of CEF. EXPANS exploits eHealth developed in other initiatives as well.

6.3 SPOCS (Simple Procedures Online for Cross-Border Services)

6.3.1 General information

SPOCS [39] aimed to build the next generation of online portals Point of Single Contact (PSC), which every European country had in place, through the availability of high impact cross- border electronic procedures.

Businesses seeking to expand into other countries often struggle to comply with all the regulations they need to follow. Applying for licences, permits and completing other administrative procedures in another country can be very complicated. SPOCS is a large-scale pilot (LSP) project that has overcome these obstacles through developing an interoperability layer for European eGovernment services online based on the existing systems of the MSs. This layer facilitates the service providers to apply via the PSC for businesses that the EU MSs have set up. Therefore, the SPOCS pilots showed that the building blocks, which composed this interoperability layer, do function in a real life environment.

At the time of writing, SPOCS has ended. The project was initiated in May 2009 and came to an end in December 2012.

16 different European countries were involved: 15 EU Member States and 1 non-EU Member State.

6.3.2 Global view

The diagram below presents a global view of the solution:

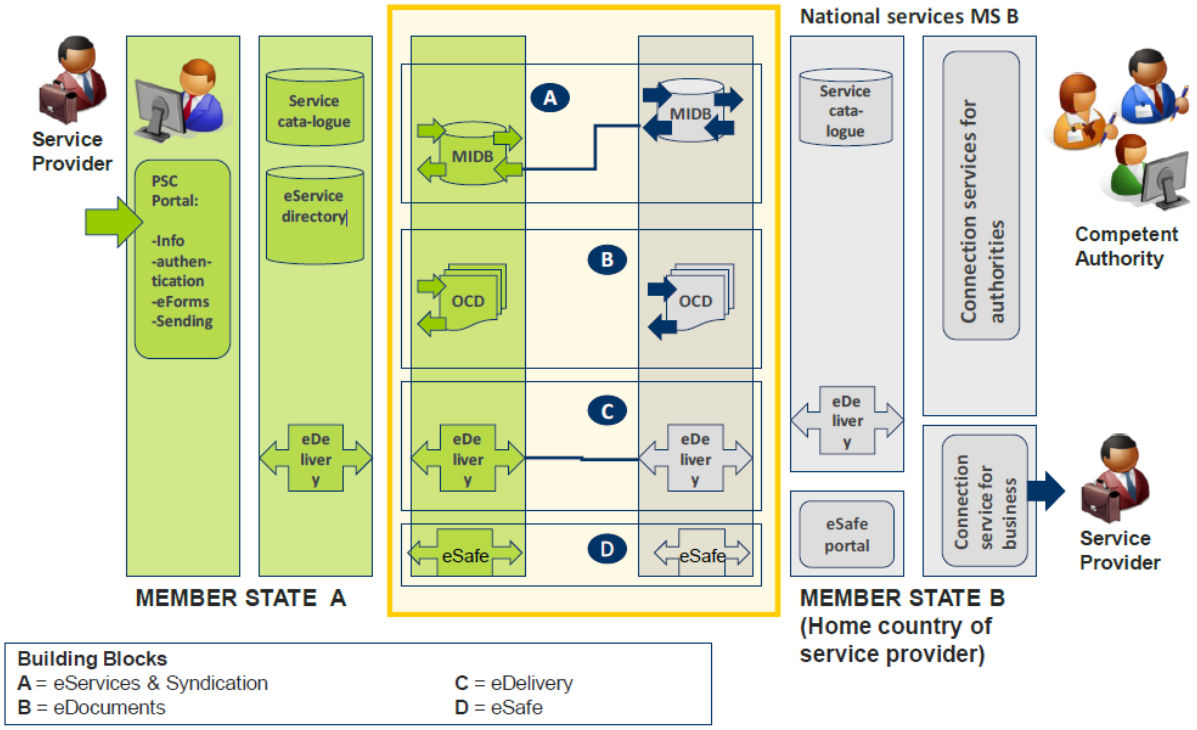


Figure 15: SPOCS global view. Source: [40]

SPOCS implements the Services Directive calls for setting up PSC, facilitating the service providers to apply via the Points of Single Contact for businesses the EU Member States have set up. The PSCs act as intermediaries between service providers and the national public administrations. The goal of these "one-stop shops" is essentially to fulfil the two following functions: information dissemination and case management/processing.

The SPOCS architecture took into account the sustainability of the solution by developing an interoperability layer based on decentralised building blocks. The building blocks have been designed for generic use case scenarios and can also be re-used in other domains where document semantic equivalence or safe transport is needed.

The architecture is decentralised based on international standards for national interfaces. However, some central components exist that provide auxiliary services, e.g. semantic mapping of documents.

The SPOCS building blocks are the following:

- Syndication: to inform the end user of a PSC which documents should be provided.
- eServices: to improve the usability of a PSC by including cross-border electronic services.
- eSafe: to enable storage and retrieval of documents safely.
- eDelivery: to asynchronously exchange electronic documents.
- eDocuments: present, sign and exchange electronic documents.

As can be seen, the PSC concept of SPOCS fits perfectly with the PEPS/V-IDP component of STORK.

6.3.3 Environment

6.3.3.1 Legal

- Directive 2006/123/EC of 12 December 2006 on services in the internal market.
- "Single Market Act II –Together for new growth" – Key Action 8 (COM(2012) 573 final, 3.10.2012).

6.3.3.2 EU projects as building blocks

The modules implemented in SPOCS considered and incorporated existing national infrastructures, by combining their positive aspects, thereby gaining the benefits of results in similar fields/topics of sibling LSP projects. The following EU solutions have been re-used in SPOCS:

- **eID** solution from **STORK** [41].
- e-Signature validation and Business Document Exchange Network solutions from PEPPOL.

SPOCS promoted the collaboration with other LSPs, as a provider of re-usable building blocks as well as a consumer of out-of-the-box solutions available from these LSPs. The following diagram shows the relationships of SPOCS with the environment of LSPs:

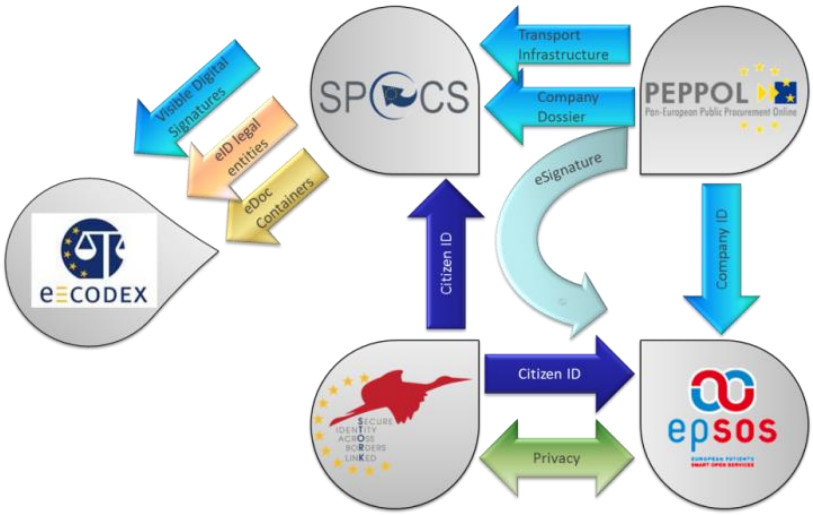


Figure 16: SPOCS LSPs collaboration activity. Source: [42]

6.3.4 Authentication

In SPOCS, identification and authentication were built upon the SAML profile of STORK [43].

6.3.5 Authorisation

The method used for establishing trust between different gateways in the network, was based on Trust-Service status List (TSL), as defined by ETSI TS 102 231 v3.1.2, which specifies the incorporation of status information for general trusted services.

6.3.6 Interoperability

SPOCS chose the **EIF** for European public services as the interoperability framework reference to specify the level of interoperability support of different system's components. On the basis of EIF, SPOCS defined a tailored interoperability framework to address all the levels of the interoperability framework: legal, organisational, semantic and technical. The following diagram shows the SPOCS interoperability framework:

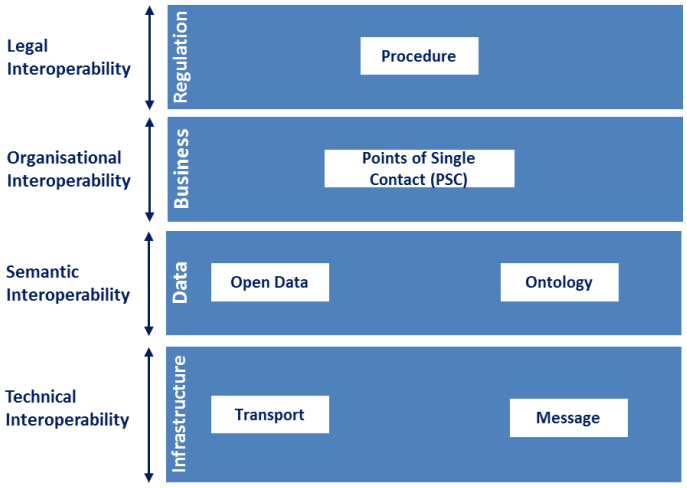


Figure 17: SPOCS Interoperability framework

SPOCS did a relevant effort regarding interoperability. The project specified five decentralised building blocks (eDocuments, Content Syndication, eDelivery, eSafe, and eService Directories) that were subjected to an open consultation among different stakeholders (MS and IT companies) [40]. **SPOCS experts worked together with international standards bodies** (ETSI ESI, ETSI TS, OCD) in order to converge standardisation efforts into these building blocks. The building blocks are published on **ISA JoinUp** under a licence compatible with the EU Public License.

Finally, it should be remarked that SPOCS established fruitful relationships with **SEMIC** in order to integrate the SEMIC **Person and Business Core Vocabularies** specification in the project data model.

6.3.7 Governance

SPOCS agreed on governance mechanisms between the MS in order to handle the information provision in the national infrastructure when needed.

SPOCS also established a **Sustainability Task Force**, which currently has no activity. This task force looked at fostering further adoption, use, and longevity of the SPOCS modules, specifications, and guidelines.

Currently, the main assets of SPOCS are maintained, extended and improved by **e-SENS**. Such e-SENS governance leadership is also in place for e-CODEX and epSOS.

6.3.8 Outcome

The results from SPOCS per se, have been packaged as a **SPOCS Starter Kit**. This package provides online information to help pinpoint the most relevant material (documents, specifications, reusable pieces of software code) that may be of interest.

6.4 e-CODEX (e-Justice Communication via Online Data Exchange)

6.4.1 General information

e-CODEX [44] aims at providing an easier and safer access to legal information and procedures in other EU Member States for citizens, legal authorities and legal professionals; automating procedures both in civil and criminal matters, strengthening cross-border judicial cooperation and providing greater effectiveness for cross-border procedures through common standards of information systems.

To this end, a service infrastructure was designed, built and tested to demonstrate the secure cross-border interoperability, which connects the existing national justice solutions. Therefore, the project had to develop common approaches and standards in several areas. Within the project, the solution was tested through working prototypes and via the piloting of several judicial use cases.

At the time of writing, e-CODEX has almost ended. The project was initiated in December 2010 and will come to an end in June 2016.

20 countries are involved, mainly through their Ministries of Justice or their representatives, and other European legal institutions.

6.4.2 Global view

The diagram below presents a global view of the solution:

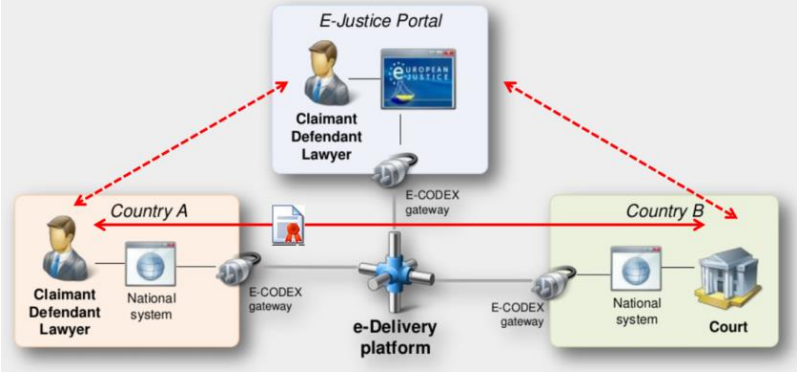


Figure 18: e-CODEX High level architecture schema. Source: [45]

e-CODEX is based on the electronic exchange of data and documents from one country to another. Thus, transport of data and documents is a key element of the solution. On top of this, the solution translates the national standards of documentation to the agreed standards within the project.

To this end, e-CODEX provides a multilateral, content agnostic e-Delivery infrastructure to develop a single pan-European interoperability layer for access to cross-border e-Justice services. These services follow agreed judicial procedures based on EU Regulations and Decisions. Mutual trust and acceptance of the national systems is needed when such cross-border electronic communication takes place.

The e-CODEX architecture is comprised of a set of building blocks: the Service Provider, the Connector, the Gateway and the e-Delivery platform. (See Figure 19 below)

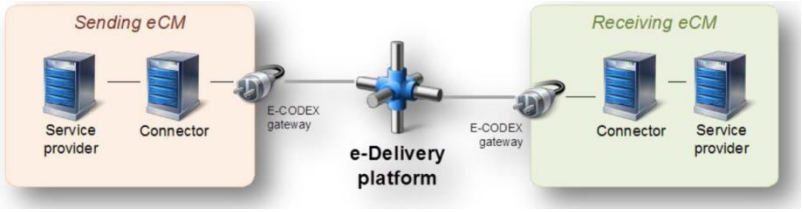


Figure 19: e-CODEX building blocks. Source: [45]

A brief explanation of each building block is introduced below:

- The Service Provider may be either a governmental or a private institution, which delivers a service in conformity with the project standards.
- The Connector transforms outgoing and incoming documents, translating between MS internal standards and project agreed standards. The latter is based on the OASIS ebXML Messaging Service (ebMS) 3.0 [46] standard.
- The Gateway is a national system for data transmission between two MS communication partners. Each MS is responsible for his own Gateway.
- The **e-Delivery** platform is responsible for the secure and reliable transport of data and files from one gateway to another. It is based on the **OASIS ebXML Messaging Service** (ebMS) 3.0 [46] standard as well.

As can be seen, the Gateway concept of eCODEX fits perfectly with the PEPS/V-IDP component of STORK.

6.4.3 EU Environment

6.4.3.1 Legal

- Multi Annual European e-Justice Action Plan 2009-2013 (2009/C 75/01).
- European e-Justice Strategy (COM(2008)329 final) .

6.4.3.2 EU projects as building blocks

The project explored collaborations and interdependencies with other EU projects [47] in order to take advantage of potential reusable components and common issues.

With regards to STORK 1.0, the following synergies were identified [48]:

- STORK already carried out about 60% of the mappings of the national solutions to the Quality Authentication Assurance (QAA) Scheme that are necessary for e-CODEX.
- The STORK QAA Scheme still allows each Member State to maintain its local definition of authentication assurance levels as required.
- The classification of the quality levels is based on assessed risks and possible damages, which proves to be a practical approach.
- STORK's work on physical entities paves the way for legal entities.
- STORK provides a data model for personal information. In addition, STORK uses code lists for country codes, gender and marital status, as far as available, using ISO standards. e-CODEX in turn, is interested in data models for the exchange of structured data.

However, STORK 1.0 was not used on the e-CODEX use cases. As with epSOS, there were some similar reasons for that [47]. Some requirements were not supported by STORK, and the project participants agreed that MS were responsible for the authentication by its infrastructure.

6.4.4 Authentication

The e-CODEX LSP use cases focused mainly on the transport of documents and data. As national solutions were meant to be accessed as a starting point, authentication should be done by each national solution itself. In terms of cross-border access, already established solutions, such as STORK, should be used to allow the cross-border usage of national authentication mechanisms. But, in the end, it was decided that the cross-border authentication of persons and entities was an optional requirement for e-CODEX (see WP4-OPT-F-003 requirement in [48]) because authentication was an integral task of the MS. Taking all this into account, e-CODEX did not provide a solution to MS A to authenticate a person or an entity of MS B and vice versa. It was agreed in e-CODEX that persons being authenticated by usage of the sending MS's national solution should be seen as authenticated within the receiving MS.

Nonetheless, e-CODEX needed some mechanism to identify the user in addition to the electronic signature because it was necessary to inform about the user's role or if the user had the required rights for a specific task. The following alternatives were analysed [48] as a means of transport of the user identity information:

- The national solution provided a business card or an equivalent document that can be attached to the message: it would require the national solutions to develop a directory that contains business cards for professionals. These business cards could include information about the role of the sender as well as his official contact information and would provide a simple means to identify and contact a professional.
- The sender's identity information was added to the message by using a **security token profile**: this was the implemented option [49]. As a standard to provide this functionality, **WS-Security** was chosen. The sender's identity information can be added to the message through security token profiles. In this regard, the **SAML Token Profile** was the standard extensible profile used to exchange the necessary identity information. Thus, the legal liability lies within the authority that authenticates the user.

6.4.5 Authorisation

Not surprisingly, as occurred with the authentication requirement, the authorisation was also considered as an optional feature in e-CODEX (see WP4-OPT-F-001 requirement in [48]). Moreover, it was decided that the validation of roles was out of scope and must be performed by the national solution. The agreed approach in the project was that the validation of the role took place in the sending MS and had to be accepted as validated by the receiving MS.

e-CODEX did not cover any process related to authorisation or validation of roles by itself, but specified the means of transporting this information. Following the same approach as with the identity information, e-CODEX allowed the **transportation of verified roles** (authorisation) information and included it as an attachment within the **SAML Token Profile** of **WS-Security**. With this approach, the legal liability remained within the authority that verified the user.

Concerning the roles mapping, due to language issues, it was found that the receiving MS would not be able to understand the verified role. So, it was recommended to implement a **role mapping at a national level** on the basis of role descriptions.

As a final recommendation, if the need for authorisation would arise as mandatory in the future, the project suggested [48] to analyse STORK 2.0 and XACML as potential base solutions.

6.4.6 Interoperability

e-CODEX chose the **EIF** for European public services as the interoperability framework reference to specify the level of interoperability support of different system's components. On the basis of EIF, e-CODEX defined a tailored interoperability framework. The following diagram shows the final interoperability layers [50] adopted by e-CODEX:

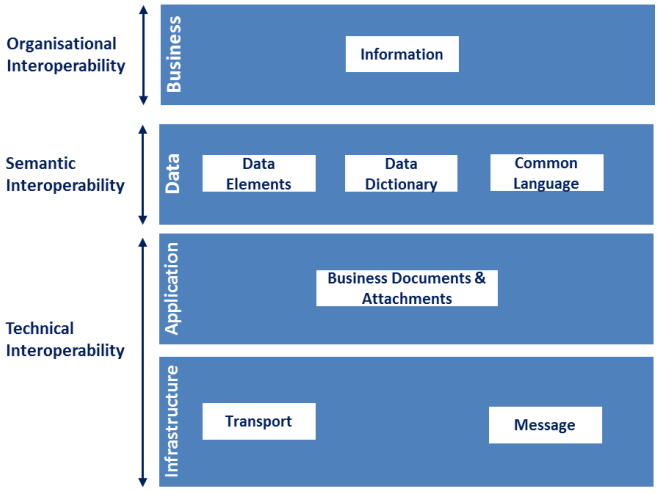


Figure 20: e-CODEX Interoperability framework. Source: [51]

Based on this framework, a set of Core Interoperability Agreements covering all 4 Interoperability Layers was defined and agreed within the project [45].

The main technical interoperability standard used in the project was the **OASIS ebXML Messaging Service (ebMS) 3.0** [46] standard.

It should be remarked that e-CODEX went one step further and created a set of interoperability solutions, which specified a **standard format of e-Documents**, and is catalogued in the ISA portal [52].

6.4.7 Governance

Along with the e-CODEX project, the governance of configuration and code base relied on a tailored TOGAF model. Once the project was ended, its governance is led by the e-SENS **e-Delivery convergence task force** [53]. This task force promotes re-usage with regards of infrastructure and components in order to avoid running different infrastructures for the different domains and converge towards a common infrastructure. It is a relevant task because the e-CODEX e-Delivery building block is expected to be widely re-used as many LSPs have the need for a platform to exchange securely documents. On the other hand, this task force integrates the overall e-SENS vision. Thus the e-Delivery platform is to be smoothly combined with building blocks from other LSP and international standards in a modular approach.

Moreover, an organisational and legal framework is currently being developed by **Me-CODEX** [54], which ensures a long mid-term sustainability of the e-CODEX major assets jointly with e-SENS.

6.4.8 Outcome

e-CODEX provided a secure and effective environment for data exchange in the field of e-Justice.

e-CODEX outcomes are **available online** [44] and released as open source software under the European Union Public Licence (EUPL) licence.

6.5 UUM&DS (Uniform User Management and Digital Signatures)

6.5.1 General information

UUM&DS project aims at enabling the provision of a unique trader interface, by implementing secure authorised access for Economic Operators (EO) and their representatives to Customs European Information Systems (EIS). UUM&DS will be a production system.

At the time of writing, factory acceptance tests have just started. The project was initiated in 2013 and it is expected to be in production in September 2017.

All the MSs are involved because the regulation imposes that all MSs implement the solution.

6.5.2 Global view

The diagram below presents a global view of the solution:

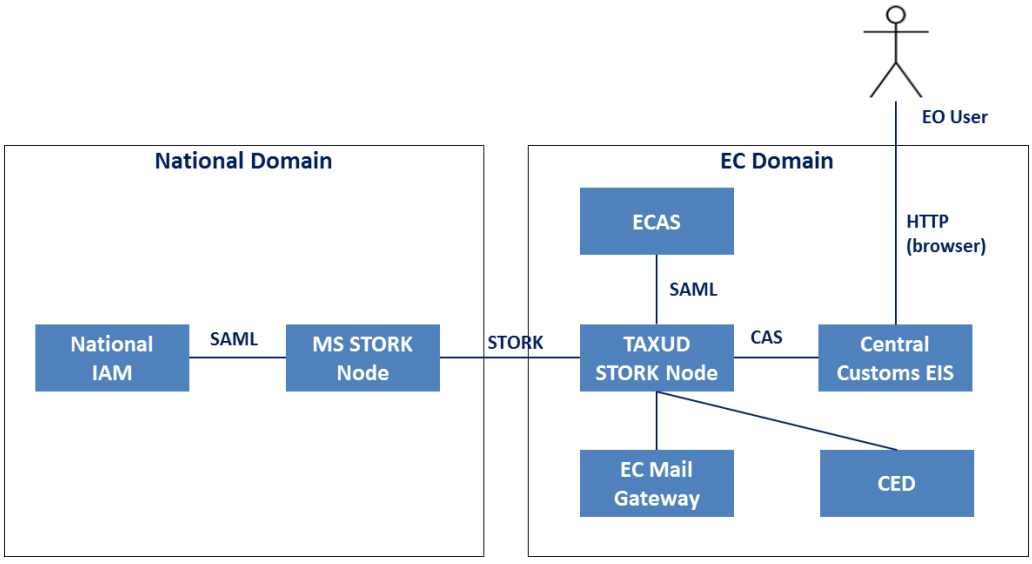


Figure 21: UUM&DS systems' domains

The implementation of the UUM&DS solution will offer direct trader access at EU level. To this end, UUM&DS will implement a federated authorisation scheme for protecting access of Economic Operators to any service of the Central Customs EIS, which will be hosted by DG TAXUD. The authorisation will be based on policies that are managed by the UUM&DS solution and the involved EU Central Customs EIS service. The solution specifies that two authorisation policy verifications will be made [55]: one coarse-grained at a central level in the UUM&DS, and another one fine-grained at a distributed level in the target service of the Central Customs EIS. In order to implement the fine-grained authorisation

verification, the Central Customs EIS will receive all the UUM&DS information (authenticated user information and permissions) through a **SAML assertion**, a **CAS assertion**, or a set of classes (UUM&DS JEE Principals).

UUM&DS will manage all the authorisation policies for all Central Customs EIS centrally. A UUM&DS policy will be composed of a set of security rules and control access of users to application services. These rules could be based on roles complemented with attributes and their mapping to actual functionalities.

The MS will manage identity information and users' attributes at a national level. MS Identity and Access Management (IAM) is the group of components of the national domain that perform the federated integration with UUM&DS. The details of this component and the interfaces used with UUM&DS may vary depending on the situation of the MSs. In this regard, UUM&DS specifies different interfaces with the MS IAM in order to support four MS integration scenarios. Three of the scenarios (which are the most important) are based on **STORK v1** and **SAML 2.0** technology. The remaining integration scenario is expected to be temporal.

Regarding authentication, although different mechanisms are supported, the recommended option is that the user choses the ECAS protocol. ECAS is the EU corporate solution for authentication. ECAS is currently integrated with STORK v1 in order to provide cross-border authentication of EC or MS officials.

When necessary, UUM&DS consults the Commission Enterprise Directory (CED) to get information about EC officials and existing ECAS accounts through the CED Consultation interface and uses the EC mail gateway to send notifications.

6.5.3 Environment

6.5.3.1 Legal

- The eIDAS Regulation of the European Parliament and of the Council [3] on electronic identification and trust services for electronic transactions in the internal market (COM(2012)0238 – C7-0133/2012 – 2012/0146(COD)).
- Use of open standards (COM (2010) 744), e.g. reusing STORK technology for federating with MS IAMs and is compliant with the corresponding EU legislative provisions.

6.5.3.2 EU projects as building blocks

UUMS&DS has a strong focus on usage of open standards and re-usage of already stablished building blocks such as **STORK** or **ECAS**.

On one hand, STORK v1 was selected for federating with MS IAMs. On the basis of STORK v1, some necessary changes were made to build a protocol extension for UUM&DS. The main changes are listed below:

- Signature (to align security with eIDAS).

- Encryption (to align security with eIDAS).
- Authentication Declaration Statement (for eIDAS compliance).
- Authorisation statement (for authorisation).
- SOAP binding for attribute query (for MS using an AP).
- Additional attributes (for customs & taxation domain purposes).

On the other hand, **ECAS** will be used and federated by UUM&DS to authenticate EC officials through the ECAS Federation interface.

6.5.4 Authentication

UUM&DS enables the cross-border recognition of identities through the federation of MS IAM systems hence allowing Economic Operators to gain access to Customs services by receiving and accepting credentials data. Thus, a user that is authenticated and authorised at the national level will be recognised in UUM&DS and the service of the Central Customs EIS.

UUM&DS supports different authentication mechanisms. However, the recommended option is that the user choses the **ECAS** protocol. ECAS is the EC corporate solution for authentication and is currently integrated with **STORK v1** in order to provide cross-border authentication of EC or MS officials.

When a user wants to access a service of the Central Customs EIS, the user is redirected to a central authentication portal. Then, the federated authentication workflow starts and the corresponding requests are forwarded between the user MS, UUM&DS and the service Central Customs EIS. Several authentication scenarios are supported through configurable parameters exchanged in the messages in order to support different integration approaches with MS IAMs.

6.5.5 Authorisation

In the context of UUM&DS, Authorisation Policy management will define the framework for organising and managing access rights to the Central Customs EIS for the different types of actors, related to information security and to access control. The authorisation policy is formalised as access control rules for the Central Customs EIS. During runtime, the system uses the access control rules to decide whether access requests from authenticated users of services (actors) shall be approved (granted) or rejected. The management and enforcement of these authorisation policies will be done centrally at UUM&DS, but user identity information is managed at a national level by MS IAMs and **federated** with UUM&DS **through STORK** technology. All the user information collected is finally forwarded to the Central Customs EIS.

In order to hide technical complexity of policy management, the authorisation policy definition will be business driven. This will be achieved by defining for the different types of actors their corresponding business profiles. The business profile encapsulates the IT application roles and their subsequent mapping to IT application permissions for specific functions and services offered by the Central Customs EIS. At MS level, the authorisation policy is implemented by assigning the business profiles to their users. Under the business profiles concept, UUM&DS defines two additional levels of rights for fine grained

access control: application roles (hidden to MS IAMs and specific to Central Service) and permissions (authorisation at technical level to allow for declarative or programmatic verification).

The authorisation policy comprises of a set of rules (criteria) for granting access to applications. If the user profile matches at least one of the rules, access will be granted. The security rule contains, inter alia, the following information:

- A list of **attributes** constraints (rule attribute).
- **Delegation** information.
- A set of **application roles** that will be granted if the user's conforms to the rule.

When receiving a request from an authenticated user for accessing a service of the Central Customs EIS, the implementation of the authorisation policy comprises of the following actions:

- Collection of authorisation-related information.
- Decision on allowing the access to a service based on this information.
- Application (enforcement) of this decision replying to this access request.

This authorisation approach of UUM&DS has similarities with principles of the **XACML** architecture (PEP, PDP, and PIP):

- MS IAMs provide the necessary user information acting as a PIP.
- UUM&DS central components could optionally act as a PIP as well. These components may complement the MS IAMs information and collect additional attributes and authorisation information (e.g. delegation and access privileges for user roles).
- UUM&DS takes the decision about granting access to the service. **UUM&DS acts as a PDP and PEP for coarse-grained authorisation decisions**, based on the collected information and the applied authorisation rules.
- Finally, the information relevant to this specific service will be forwarded to the Central Service so that it can take context-specific (data centric) decisions on user's request for accessing specific data sets and implementing fine-grained authorisation based on the received authorisation information without the need to consult UUM&DS.

This model will allow for parametric, dynamic, easily-maintainable and user-friendly authorisation policy management.

Finally, it should be noted that the UUM&DS authorisation policy is not only business driven but also data centric because it embraces the RBAC approach combined with the ABAC mechanism.

6.5.6 Interoperability

UUM&DS is compliant with the **EIF**. This is a mandatory requirement for the system.

The EIF compliance is assured on the basis of a major component compliance, STORK. **STORK** is compliant with EIF. Therefore UUM&DS PEPS are compliant as well.

Finally, the design of the UUM&DS system has a strong focus on the use of open standards. This is a system requirement as well.

6.5.7 Governance

At the time of writing, no information is available.

6.5.8 Outcome

It should be noted that the UUM&DS project is still progressing. Therefore, the outcomes elaborated below are valid at the time of writing. Additional topics may arise as the project moves forward.

On the basis of the UUM&DS Authorisation approach, we can draw some **parallelism between the UUM&DS authorisation and XACML**:

- The UUM&DS solution is based on Policy Enforcement Point/Policy Decision Point/Policy Information Point concepts, which in turn, are the basis of the XACML architecture.
- The UUM&DS solution supports the definition of policies, rules, and permissions. These definitions could be done also with XACML.
- The UUM&DS solution proposes exchanging the authorisation information with SAML.

The UUM&DS project decided to re-use the XACML terminology and features as much as possible because they are easy to understand. It was also taken into account that the XACML security concepts are valid and widely accepted in federated environments.

However, the **XACML specification per se was not used** in the UUM&DS project. XACML was discarded on the basis of the feasibility study for the following reasons, inter alia: not supported in any MS, no experience/expertise available in MS, and introduces some complexity.

Finally, taking into account the new eIDAS regulatory and technical environment, if the project started at the time of writing, an assessment should have been done to determine the best fit-for-purpose solution with regards to the underlying authentication framework. The proposed solution in UUM&DS is based on STORK v1 to promote EU building blocks re-usage and sustainability. At the time of doing the selection, STORK v1 was the best option, but at the time of writing, the context is different and it is foreseen that STORK may disappear.

6.6 STORK 2.0 pilot 3 (eGovernment for business)

6.6.1 General information

The STORK 2.0 pilot eGovernment for business [56] established the connection of business registers to the national STORK 2.0 nodes, and cross-border piloted this connection, allowing businesses to establish foreign branch offices.

Businesses seeking to expand into other countries often struggle to comply with all the regulations they need to follow. Applying for licences, permits and completing other administrative procedures in another country can be very complicated.

6.6.2 Global view

The global view of this pilot is the same as the one in STORK. (See section 5.2.2).

6.6.3 Environment

6.6.3.1 Legal

The legal environment of this pilot is the same as the one in STORK. (See section 5.2.3.1).

6.6.3.2 EU projects as building blocks

The EU environment of this pilot is the same as the one in STORK. (See section 5.2.3.2).

6.6.4 Authentication

STORK 2.0 has defined the *Authentication on behalf of* process flow, which has been used in this pilot to allow natural persons to open a foreign branch office on behalf of a company. The mandate can be chained, e.g. a business can mandate a lawyers' office, which in its turn mandates one lawyer to represent the business.

The legal person's identity is contrasted with the business register, and the powers of representation (mandate) is also checked against this register.

6.6.5 Authorisation

The authorisation is performed by the application, based on the retrieved mandate. The most common typeOfPower is the "general powers", which in most cases could be machine-interpreted.

6.6.6 Interoperability and standards

No internationally accepted standard exists for mandates. Some countries have categories of types of mandates, but those categories have been found to be insufficiently similar.

6.6.7 Outcome

The STORK 2.0 results and governance are detailed in section 5.2.9. The main achievement of this pilot is proving that cross border mandates can be used.

6.7 STORK 2.0 pilot 4 (eHealth)

6.7.1 General information

The STORK 2.0 pilot for eHealth established [57] the connection of the STORK authentication with the epSOS NCP nodes, and cross-border piloted this connection, allowing patients, Healthcare Professionals as well as representatives of the patient to retrieve the patient's data in a foreign country.

The executive summary of its deliverable D5.4.5 eHealth pilot Final Report, [57] highlights that "the STORK 2.0 eHealth pilot has increased transparency, security and efficiency in cross-border eHealth and this is demonstrated through the following pilot achievements:

- "STORK 2.0 eID infrastructure is used for secure eID and authentication to access the epSOS eHealth infrastructure and to thus build a bridge between the two domains of eGovernment-IDs and eHealth-IDs.
- Enables patients to access their health data in their home country and in foreign countries using their local eID mechanisms.
- Supports mandates such as patients delegating their rights to someone else. Expanding the standard role-based situation with healthcare professionals (organisations or natural persons) acting on behalf of patients, the pilot allows for explicit representation by other persons such as family members or lawyers. Representations can be restricted for certain purposes or time periods.
- STORK 2.0 is used as a source of user attributes from local health IT-infrastructures and can be used to authorise users as Health Care Providers."

The eHealth pilot achieved important synergies between the eHealth and the eGovernment sector by using the STORK eID infrastructure as the secure eID and authentication means to access the epSOS eHealth infrastructure between Italy, Austria, Switzerland and Turkey. It should be mentioned that Turkey did not participate in production tests because of national data protection regulations with real patients data. The pilot deployed all three eHealth fundamental use cases in production in over five 'live' services (pilot details and outcome are available at [57]):

- Authentication of the patient. This use case was successfully piloted between Austria, Italy and Turkey.
- Authentication of another person on behalf of the patient. This use case was successfully piloted between Austria, Italy and Turkey.
- Authentication of the healthcare professional accessing the patient's data. This use case was successfully piloted in Austria.

6.7.2 Global view

The global view of this pilot is the same as the one in STORK (see section 5.2.2), combined with the NCPs as illustrated in section 6.2.2.

6.7.3 Environment

6.7.3.1 Legal

The legal environment of this pilot is the same as the one in STORK (see section 5.2.3.1), combined with the epSOS legal environment as described in 6.2.3.1.

6.7.3.2 EU projects as building blocks

The EU environment of this pilot is the same as the one in STORK (see section 5.2.3.2), combined with the epSOS building block as described in 6.2.3.2.

6.7.4 Authentication

STORK 2.0 has defined the *Authentication on behalf of* process flow, which has been used in this pilot to allow natural persons to retrieve a patient's information on behalf of this person. It has also piloted the role-based authorisation using the isHealthCareProfessional attribute.

6.7.5 Authorisation

The authorisation is performed by the NCP where the data are stored, based on the retrieved mandate in use case 3 (a person mandated by another person). In the other use case, the authorisation is also done by the NCP, based on the role of the Healthcare Professional.

6.7.6 Interoperability and standards

No internationally accepted standard exists for mandates. Some countries have categories of types of mandates, but those categories have been found to be insufficiently similar.

For the isHealthCareProfessional attribute, its sub-attributes *typeOfOrganisation* and *typeOfHCP* have assumed the semantic values from epSOS, maximising the interoperability between both platforms.

6.7.7 Outcome

The STORK 2.0 results and governance are detailed in section 5.2.9. The main achievement of this pilot is proving that cross border mandates can be used, offering the following to European citizens and healthcare professionals:

- Enables patients to access their health data in their home country and in foreign countries using their local eID mechanisms.
- Supports mandates such as patients delegating their rights to someone else. Expanding the standard role-based situation with healthcare professionals (organisations or natural persons) acting on behalf of patients, the pilot allows for explicit representation by other persons such as

family members or lawyers. Representations can be restricted for certain purposes or time periods.

- Allows healthcare professional's technical access to foreign patients' patient summaries in a "break the glass" scenario (for example, when a patient is unconscious and the healthcare professional needs access to the patient summary without formal consent by the patient, depending on the legal situation).

6.8 Findings

From the domain specific projects the following findings have been extracted:

Description	Field of influence	Source
MS participation was crucial for the sustainability of the cross-border domain specific solutions, but **universal MS participation was not achieved** in any LSP. It is recommended to enlist as much collaboration as possible from all the stakeholders.	Recommendation	All
Set up an **interoperability layer based on EIF** to allow for communication between the national infrastructures. This ensures more protection of the MS investment (they don't need to completely change the national infrastructure) and attracts the adaptations and reuse of the interoperability layer for cross-border exchanges.	Recommendation	All
Configuration and information provisioning of the national infrastructure was based on mutual trust and internal project agreements.	Experience	All
The building blocks, cross-border systems and messages were designed to **interfere as little as possible** into national infrastructure.	Recommendation	All
The **national regulation was respected**. Projects specifications were flexible enough to allow that national dependent processes (because of national constraints or regulations) can be done in the MS infrastructure. Solutions should provide different configurable options for these processes to be fully **compliant with both European and national requirements**.	Recommendation	All
Promote the usage of standard data models.	Recommendation	SPOCS (SEMIC Core Vocabulary),

Description	Field of influence	Source
		epSOS (IHE profiles)
Authentication mechanism relies on the existing national authentication solutions. Irrespective of the national eID solution, the domain specific projects achieved successful eID integration.	Recommendation	epSOS, e-CODEX
Authentication mechanism relies on STORK. Finally, all the projects, with the exception of e-CODEX, demonstrated the feasibility of reuse STORK as eID platform.	Experience	SPOCS, UUM&DS, STORK 2.0 pilot 3 and pilot 4 (based on epSOS)
Authorisation is based on attributes.	Experience	All except UUM&DS
Authorisation is based on policies.	Experience	UUM&DS
Adoption of XACML authorisation concepts (but not implemented).	Experience	UUM&DS
The solutions were successfully deployed following a federated approach, where each MS has a single point of access (acting as a gateway) for the other MS.	Experience	All

Table 3. Domain Specific Projects - Major findings

7 Potential Solutions

This chapter describes the potential solutions identified for federated authorisation in the context of ISA Action 1.18. The description includes functional, technical and governance details along with its advantages and drawbacks.

7.1 Requirements and Assumptions

7.1.1 Assumptions

The definition of Action 1.18 implies several assumptions or prerequisites, which make certain possible solutions unfeasible. The following table describes these assumptions and their consequences.

ID	Assumption	Description	Consequence
AS1	Authorisation decisions are taken by the MS	Public officials should be granted access to EC applications by their national administration.	The role a public official has in his/her organisation can't be used by the EC to map the authorisation to access EC applications.
AS2	Administration of authorisation decisions	The administration of authorisation decisions is performed by each MS, and is reflected in its own repository.	The MS are responsible of mapping, within their distributed national infrastructure, of their national roles to the specific roles of the EC applications.
AS3	The proposed solution should fit in STORK and eIDAS	The proposed solution should be compatible with STORK and also with eIDAS. Currently, the MS have STORK eID nodes but it should be taken into account that before September 2018, the MS have to be eIDAS compliant.	Irrespective of the MS decision concerning their strategy towards the eIDAS compliance in 2018, the proposed solution should be respectful of STORK and eIDAS. It is expected that both STORK and eIDAS may require small changes to support this solution, but will anyway be used to transport the authorisation information.

Table 4. Assumptions for the federated authorisation solution

7.1.2 Requirements

The following requirements have been derived from the analysis conducted in Phase 3 of Action 1.18, and collected from Previous Phases of Action 1.18:

ID	Request	Description	Source
RQ1	A federated authorisation solution should be proposed.	A federation-based authentication and authorisation mechanism should be established, in order to avoid the overhead of managing users at national level for internal needs and at ECAS level for EC Applications.	ISA Action 1.18
RQ2	Processing of personal data shall be carried out in accordance with Directive 95/46/EC.	The directive 95/46/EC describes principles of protection of the privacy of personal data.	Directive 95/46/EC, eIDAS Regulation
RQ3	The solution should be technology neutral.	As the solution should fit into the eIDAS and STORK infrastructure (AS3), which are technology-neutral, this requirement will be met.	eIDAS Regulation
RQ4	The solution should follow European and international standards, where possible.	European and international standards have been studied on their requirements for the solution to be proposed.	eIDAS Regulation
RQ5	The solution should not discriminate between any specific national technical solutions for electronic identification within a MS.	As the solution should fit into the eIDAS and STORK infrastructure (AS3), which don't discriminate, this requirement will be met.	eIDAS Regulation
RQ6	The solution should facilitate the implementation of the principle of privacy by design.	As the solution should fit into the eIDAS and STORK infrastructure (AS3), which facilitates the privacy by design, this requirement will be met.	eIDAS Regulation
RQ7	The solution should ensure the interoperability of the	As the solution should fit into the eIDAS and STORK infrastructure (AS3), which ensures cross-border eID interoperability, this	eIDAS Regulation

ID	Request	Description	Source
	electronic identification schemes.	requirement will be met by the underlying infrastructure. The solution should maintain such interoperability.	
RQ8	The solutions should be compliant with legal restrictions.	The federated authentication solution should comply with national and EU level regulations, in particular, concerning the transmission of personal information (attributes).	Previous Phase
RQ9	The solution should support cross-border and cross-sector usage.	Any solution elaborated within the ISA programme, should be usable in all EU countries for cross-border interchange of data.	ISA programme

Table 5. Requirements for the federated authorisation solution

7.2 Technical solutions

7.2.1 Authorisation attribute

7.2.1.1 Description

This solution is based on using a **new attribute**, named **Authorisation**, which will hold information about the roles that the user has granted access in the EC application. The EC application will use the information received within this attribute to make the access control decision. This attribute provides application and role information which has been stored and managed in the national infrastructure.

This new attribute should follow the request/response rules of the **SAML 2.0 AttributeStatement**.

The Authorisation attribute should be defined as a new type that includes two sub-attributes: <application> and <role>. The Authorisation attribute can contain more than one discrete value. In order to improve the user experience, taking into account the Single Sign-On (SSO) feature of ECAS, it is recommended that the MS provide all the application/role pairs of the EC applications to which the user's access is granted.

Following the approach of the eIDAS SAML profile, the specification of such Authorisation attribute should be created as a **new authorisation specific XML schema**, which would contain the definitions of authorisation attributes (role and application in this particular case). In order to assure compatibility with eIDAS, this new schema **should be created following the eIDAS Technical Sub-group guidelines** and its

attributes should be exchanged through the eIDAS domain specific part, as stated in the eIDAS SAML Message Format specification [58]. This approach means that all MS, where a custom attribute is relevant, such as the authorisation one, can implement the new custom attribute, while the other MS can decide not to support it, removing the necessity to change the whole eID infrastructure any time a new required attribute would emerge.

This new schema should be maintained by an authorisation (or security) expert group. It is advised that the eIDAS Technical Sub-group would play a "sense checking" role prior to publication of any schema change. This would ensure that duplication across domain specific attribute sets is minimised and that the encoding of data is as consistent as possible across the MS federation.

7.2.1.2 Advantages and drawbacks

Advantages
Ease of implementation in eIDAS and STORK infrastructure. In the eIDAS SAML a minimal dataset is defined and all MS must implement the minimum dataset. To exchange other information, such as the new Authorisation attribute, the eIDAS SAML has a sector specific part where anyone can pass through any custom attribute. This approach means that all MS, where a custom attribute is relevant, can implement the new custom attribute, while the other MS can decide to not implement it, removing the necessity to change the whole infrastructure any time in any domain a new required attribute would emerge. STORK also supports the exchange of domain specific attributes. It is recommended to request the attribute as optional to avoid error messages from MS that don't implement this attribute. e-SENS reported that handling new custom attributes was too heavy concerning governance and implementation.
Compatibility with existing standards. Although it has not been tested, the project team expects such a new attribute to be "interoperable" with the eIDAS SAML profile. As this new attribute should be packaged within an authentication response in the corresponding attribute statement, it is expected that STORK/eIDAS nodes which don't understand this new information will ignore it. This means that nodes that don't understand such (parts of the) messages will operate normally, although not using this attribute.
Readiness. Since it is foreseen that the necessary code changes would be minor, the updated components would be ready in the short-term.
Reference implementations. Piloted in STORK, STORK 2.0 and Previous Phase of ISA Action 1.18.

Table 6. Authorisation attribute technical option - Advantages

Drawbacks
Not strictly conformant with the SAML standard with regard to authorisation. SAML specifies the AuthzDecisionStatement for transmitting authorisation decisions. Thus, the use of the SAML AttributeStatement for authorisation purposes doesn't conform strictly to the SAML standard usage.
Governance. Since it is based on a custom attribute, the governance could be complex because the agreements should be accepted by all MS, not by an individual organisation if it was a standard attribute. Also the medium-long term sustainability could be an issue because the complexity of maintenance of possible custom values and its meaning increases over time.

Table 7. Authorisation attribute technical option - Drawbacks

7.2.2 Mandate attribute

7.2.2.1 Description

This solution is based on using an attribute, named **Mandate**, present in STORK but new in eIDAS, which will hold information about the user mandates on EC applications. A mandate is a bundle of authorisations granted by an entity to the user to perform well-defined actions with legal consequences in the name of the former. The EC application will use the information received within this attribute to allow or deny access to its functions. This mandate information will be stored and managed in the national infrastructure.

This attribute should follow the request/response rules of the **SAML 2.0 AttributeStatement statement**.

It should be remarked that the mandate concept is a complex issue that was firstly addressed in STORK 2.0, and will be further developed in the next **ISA² Action, "Semantic Interoperability for Representation Powers and Mandates"**, in the sense that a new **SEMIC Core Vocabulary** with the Mandate specification will be produced. Hence, the details of the Mandate attribute cannot be provided at this moment.

Following the approach of the eIDAS SAML profile, the specification of such Mandate attribute should be created as a **new authorisation specific XML schema**, which would contain the definitions of authorisation attributes (mandates in this particular case). In order to assure compatibility with eIDAS, this new schema **should be created following the eIDAS Technical Sub-group guidelines** and its attributes should be **exchanged through the eIDAS domain specific part**, as stated in the eIDAS SAML Message Format specification [58]. This approach means that all MS, where a custom attribute is relevant, such as the authorisation one, can implement the new custom attribute, while the other MS

can decide not to support it, removing the necessity to change the whole eID infrastructure any time a new required attribute would emerge.

Once the Mandate data model specification would be defined by the ISA² Action, "Semantic Interoperability for Representation Powers and Mandates", its attributes could be included in such new specific schema. It is foreseen that the "type of powers" concept should have a tree structure, on its lowest level including information of the EC applications and roles that the user has granted access. Such authorisation data (EC application and roles) is the same as the one exchanged in the ApplicationRole potential solution.

This new schema should be maintained by an authorisation (or security) expert group. It is advised that the eIDAS Technical Sub-group would play a "sense checking" role prior to publication of any schema change. This would ensure that duplication across domain specific attribute sets is minimised and that the encoding of data is as consistent as possible across the MS federation.

7.2.2.2 Advantages and drawbacks

Advantages
Ease of implementation in eIDAS and STORK infrastructure. In the eIDAS SAML a minimal dataset is defined and all MS must implement the minimum dataset. To exchange other information, such as the new Mandate attribute, the eIDAS SAML has a sector specific part where anyone can pass through any custom attribute. This approach means that all MS, where a custom attribute is relevant, can implement the new custom attribute, while the other MS can decide to not implement it, removing the necessity to change the whole infrastructure any time in any domain a new required attribute would emerge. STORK also supports the exchange of domain specific attributes. It is recommended to request the attribute as optional to avoid error messages from MS that don't implement this attribute. The Mandate attribute already exists in STORK, although the permitted values of typeOfPowers should be reviewed.
Compatibility with existing standards. Although it has not been tested, the project team expects such a new attribute to be "interoperable" with the eIDAS SAML profile. As this new attribute should be packaged in an authentication response, it is expected that STORK/eIDAS nodes which don't understand this new information will ignore it. This means that nodes that don't understand such (parts of the) messages will operate normally, although not using this attribute.
Compatibility with SEMIC Core Vocabularies. The upcoming ISA² Action, "Semantic Interoperability for Representation Powers and Mandates", will specify an agreed data model definition of Mandates and Powers as a part of the SEMIC Core Vocabularies. This specification of the Mandate is foreseen to be ready on Q2/2017. Thus, the compatibility with Core Vocabularies will be achieved in the short-term.

Advantages
Governance. Since the new attribute would be based on such a SEMIC Mandate specification, the coherence assurance of the schema would be easier. Hence, the governance and its sustainability will be easier as well.
Reference implementations. Piloted in STORK 2.0.
MS need. The MS have already requested to the EC to proceed with a Mandate specification because it is a concept needed by many cross-border services.

Table 8. Mandate attribute technical option - Advantages

Drawbacks
Not strictly conformant with the SAML standard with regard to authorisation. SAML specifies the AuthzDecisionStatement for transmitting authorisation decisions. Thus, the use of the SAML AttributeStatement for authorisation purposes doesn't conform strictly to the SAML standard usage.
Debate on the legal feasibility and semantic suitability of using Mandates for authorisation purposes. Mandates are a complex issue because they have legal implications and their scope is broader than authorisation. Mandates will be studied in eIDAS because each MS understands/implements them in a different way and there's a need of common understanding. Technically speaking, a Mandate attribute can be exchanged and interpreted seamlessly for authorisation purposes. However the adoption of Mandates for authorisation purposes could be **questionable at functional and legal level**. The Mandate "on behalf of" situation is quite different of just a role linked to an application. It could introduce possible issues mixing up the legal concepts of "A representing B" with role and application. Thus, an in depth analysis would be necessary to balance all the pros and cons for such Mandate usage. As example of potential Mandate misuse, the Spanish case could be mentioned. In Spain public officials don't have Mandates, so using the mandate attribute could be considered as an abuse of this attribute. The upcoming ISA² Action, "Semantic Interoperability for Representation Powers and Mandates", should take care of the definition of their scope and meaning. Finally, it should be mentioned that there are not many MS which have attribute providers which can deliver a Mandate for a person.

Drawbacks
Readiness. Since the new Mandate definition should be provided by another ISA² Action (2016-2018), the updated components would be ready in the medium term. Also, there are not many MS which have attribute providers which can deliver a Mandate for a person.

Table 9. Mandate attribute technical option - Drawbacks

7.2.3 Authorisation decision

7.2.3.1 Description

This solution is based on using a new type of statement, complementary to the AuthnStatement and the AttributeStatement, within the assertion which transfers the result of the authorisation decision. The authorisation decision information will be used by the EC application straightforwardly. Hence, in this particular case, the EC application will not determine if the user is authorised or not. It will simply apply the decision received. This authorisation decision should be determined by a new component of the federation.

This new statement should follow the rules of the **SAML 2.0 AuthzDecisionStatement statement**.

The AuthzDecisionStatement has a single value which is the permission to access the requested application in a certain role. In order to improve the user experience, it is recommended to include the complete set of applications the user is allowed to access in the response. This way, the SSO feature of ECAS will avoid being redirected to his/her country for each application he/she accesses.

This solution would have two major consequences:

1. The eIDAS SAML and the STORK specifications should be changed to allow the exchange of AuthzDecisionStatement tokens. The current eIDAS SAML Message Format specification, as per version 1.0 [58], does not mention the AuthzDecisionStatement token. Strictly speaking, the eIDAS specification does not force that the node implementations allow to exchange any other token different from AuthnStatement or AttributeStatement. The same applies for the STORK 1.0-2.0 specifications, they should be changed to clearly state that the AuthzDecisionStatement token exchange has to be supported by the nodes.
2. The need of a new component that determines the authorisation decision.

Unlike the solutions based on attributes, this solution does not require the creation of a new specific schema.

7.2.3.2 Advantages and drawbacks

Advantages
Strict conformance with the SAML standard with regard to authorisation. SAML specifies the AuthzDecisionStatement for transmitting authorisation decisions. Thus, this is to be considered as an adequate authorisation solution. It is also in the eIDAS style: eIDAS separates the authentication statement from the attribute statement. So one more type of statement would be the correct solution.
Reference implementations. UUM&DS project implements this option. It is expected to be in production in September 2017.

Table 10. Authorisation decision technical option - Advantages

Drawbacks
Difficult of implementation in eIDAS and STORK infrastructure. The eIDAS and STORK specifications have to be reviewed in order to explicitly allow for the new type of assessment, AuthzDecisionStatement, in the SAML message.
Compatibility with existing standards and implementations. The project team expects such a new SAML statement not to be exchanged by the current eIDAS/STORK implementations. As this new type of assertion should be packaged in an authentication response, it is expected that the transaction fails in the eIDAS/STORK nodes which will reject the SAML message because is not strictly conformant with the eIDAS/STORK specifications. This is due to the fact that the eIDAS SAML Message Format 1.0 and the STORK 1.0-2.0 specifications don't mention the AuthzDecisionStatement token. Thus, strictly speaking, the eIDAS/STORK node implementations are not forced to allow the exchange of any other SAML token different from AuthnStatement or AttributeStatement. Thus, a message with an AuthzDecisionStatement token could be rejected depending on the eIDAS implementation. In fact, the current reference eIDAS implementation performs strict message validation and would most probably reject the whole message. To overcome this drawback, the eIDAS SAML and the STORK 1.0-2.0 specifications should be changed to allow the exchange of AuthzDecisionStatement tokens.
Need for a new component that determines the authorisation decision. The AuthzDecisionStatement assertion is a new element that should be included in the SAML message when requesting the authorisation. Such inclusion in the assertion should be done by a new component that should be aware of the

Drawbacks
authorisation information, decide according to the user access request and introduce the new SAML statement result in the message.
Governance. At the time of writing, there's only one EU project (UUM&DS) that has established a governance process for managing policies that support the information needed to decide on the AuthzDecisionStatement result. The UUM&DS governance experience could be used as a starting point, but the governance and sustainability of the Authorisation decision solution could be complex because is not based in standard authorisation policies.
Readiness. Since a new component is necessary, its readiness is expected in the medium term.

Table 11. Authorisation decision technical option - Drawbacks

7.2.4 Usage of XACML

7.2.4.1 Description

This solution is the most academic one, because it is based on using the architecture and access control policies specifications of **XACML**, which is the reference authorisation standard.

XACML has a specific SAML profile, named SAML 2.0 profile of XACML v2.0 [21], to facilitate the exchange of authorisation information through SAML nodes. Thus, in principle, the STORK/eIDAS nodes could support this approach.

However, it would be necessary to implement some additional **XACML components such as Policy Enforcement Point (PEP), and Policy Decision Point (PDP)** as a minimum, and include the XACML authorisation decision in the eIDAS/STORK specifications and implementations.

The EC application will receive the authorisation decision information, which can be used directly such as that with the "Authorisation decision" solution. The authorisation decision should, firstly, be enforced by the **PEP (located at ECAS)** and, secondly, decided by the **PDP (located at the MS)**. These are new components to be developed in the federation. The PDP component will decide if the user has granted access on the basis of the configured policies rules. The policies rules follow the XACML access control policies specification.

In order to ensure compatibility with eIDAS, this new schema should be created following the eIDAS Technical Sub-group guidelines and its attributes should be exchanged through the eIDAS domain specific part, as stated in the eIDAS SAML Message Format specification [58].

The authorisation decision transmitted with XACML is simple because no multiple values are allowed. So, unless the MS supports a SSO feature, the user needs to authenticate each EC application he accesses.

7.2.4.2 Advantages and drawbacks

Advantages
Strict conformance with a standard (XACML) with regard to authorisation. XACML is the reference standard for authorisation. The XACML model is conceptually an excellent model for the communication of authorisation decisions to applications.
Easy Governance. Since it would be based on an authorisation standard attribute, the governance and sustainability are expected to be easy.

Table 12. XACML technical option - Advantages

Drawbacks
Difficult of implementation in STORK/eIDAS. This solution needs the mapping of two standards (e.g. XACML and SAML) in a way that is compliant with STORK and eIDAS specifications.
Need for new components that implement the XACML architecture. Several components are needed to realize the XACML specification such as PEP, PDP, etc. Some of these components could be built on top of the eIDAS components, but many changes are needed. Also, implementing XACML complementary to SAML increases the complexity.
Compatibility with existing standards. A specific schema should be created. This schema should not only be based on the eIDAS SAML profile, but also be compatible with the XACML – SAML profile. It is foreseen that the specification of this new schema could be complex, because it means the mapping of two profiles: XACML with eIDAS SAML through the XACML – SAML profile. Also, this dependency on the SAML profiles may introduce some coupling. In the future, if the eIDAS SAML profile changes, it should be verified if the new schema of this solution continues being eIDAS compliant.
No reference implementations. At the time of writing, no reference implementations are known at EU level.

Drawbacks
The UUM&DS project has reused parts of the XACML model in the specification of the solution, but not the specification per se. UUM&DS evaluated the feasibility of using XACML, but only some conceptual parts were re-used.
Readiness. Since several new components are necessary, the readiness is expected in the medium-long term.

Table 13. XACML technical option – Drawbacks

7.2.5 Comparison of advantages and drawbacks

Concepts analysed as advantages and drawbacks	Authorisation attribute	Mandate attribute	Authorisation decision	XACML
Technical concepts				
Ease of implementation in eIDAS	✓	✓	✗	✗
Ease of implementation in STORK	⚠	✗	✗	✗
Strict conformance with a standard with regard to authorisation	✗	✗	✓	✓
Compatibility with SEMIC Core Vocabularies	✗	✓	✗	✗
Compatibility with existing standards	✓	✓	✓	✗
No need for new component(s)	✓	✓	✗	✗
Easy mapping with eIDAS	✓	✓	✓	✗
Reference implementations	✓	✓	✓	✗
No debate on legal feasibility nor semantic suitability	✓	✗	✓	✓
Sustainability concepts				
Readiness	✓	✗	✗	✗
Governance	✗	✓	✗	✓
Specific need requested by MS	✗	✓	✗	✗
Percentage of accomplishment				
	63%	67%	42%	25%

Table 14. Summary of advantages and drawbacks of the potential solutions

It should be noted that all concepts have equal weight in the calculation of accomplishment.

7.2.6 Summary of the comparison

Four technical options have been identified and analysed. All of them are **conformant with the SAML 2.0** standard, which is the core standard used at the STORK/eIDAS specifications. All of them have **benefits but also drawbacks** that have been already explained in detail in the previous sections. All of them are **feasible except the XACML** option which implies a major impact because its underlying model needs the implementation of new components.

The advantages and drawbacks have not been weighed. On the contrary, the benefits and drawbacks have been described in an objective way, giving the same importance to all the concepts and only providing reliable and truthful information.

Technically speaking, the first two options are very similar, which is to use a custom attribute, the Authorisation or the Mandate. Their major benefit is the easy inclusion in the eIDAS/STORK specifications and implementation. As a common drawback, it should be noted that e-SENS reported that handling new custom attributes was too heavy concerning governance and implementation.

On one hand, the **Authorisation attribute** option is based on custom properties that have to be defined and agreed. Hence, it can be anticipated that some governance/sustainability issues may arise not only in the short term but also in the medium-long term. A major benefit of this option is its simplicity, since it can be easily adopted by the MS with low impact with regards to implementation.

On the other hand, it is envisaged that the **Mandate attribute** option would be based on the upcoming SEMIC Core Vocabulary related to mandates. The Mandate concept is to be further developed in the next ISA² Action, "Semantic Interoperability for Representation Powers and Mandates", which is expected to produce a new SEMIC Core Vocabulary for Mandates and Powers. Among other challenges, this ISA² Action should deal with the process of refining the tree of type of power until the level of permission to access an application is reached. By being based on a standard, the governance and sustainability of this option is expected to be easier than the Authorisation attribute option. However, the Mandate option readiness is less than the Authorisation attribute because: firstly, this Mandate Core Vocabulary still has to be defined, and secondly, it has to be piloted and implemented. Finally, there is currently an open debate on the legal, semantic and functional feasibility of using Mandates for authorisation purposes. It should be analysed if the usage of Mandates for authorisation purposes is appropriate and accurate.

Both attribute based options, Authorisation and Mandate, aren't strictly conformant with the OASIS standard with regard to authorisation. The reason for this is that SAML, with its AuthzDecision design, and XACML are the per se standards for exchange of authorisation information. However, both have reference implementations of cross-border authorisation usage in EU pilots.

Concerning the **Authorisation decision** option, it is conformant with the SAML standard and its authorisation approach. However, its major drawback is the effort it may require to implement it in the eIDAS/STORK specifications and implementations, because new components are necessary with this option.

It should be mentioned that the first 3 technical options have production-ready reference implementations. As such, STORK 2.0 pilots are currently in production, with SAML attribute based authorisation implementations, and the UUM&DS system will be in production in September 2017 with SAML AuthzDecisionStatement as the authorisation method.

Regarding the **XACML** option, the final recommendation is to **discard this option**. This option conforms to the standards, but compared to the others, the integration effort in the eIDAS/STORK specifications and implementations would be much more because standards mappings should be done and new

components are necessary. Furthermore, the lack of experience in any EU MS with such a solution is a major drawback as well. On top of this, the user experience of this solution is expected to be much worse than in the first three options, as it is designed for individual authorisation requests, so it wouldn't support the Single Sign-On feature of ECAS. As compared to the other options, it has no advantages, but many drawbacks.

Finally, it should be remarked that **the first 3 technical options are not mutually exclusive**. Hence, the federated authorisation solution could support seamlessly that the authorisation is finally implemented through any of these options according to the MS needs. In practice, the following changes should be done in the STORK/eIDAS implementations to support seamlessly these 3 authorisation options:

- Allow the exchange of the additional SAML authorisation tokens (e.g. authorisation decision) in the intermediate nodes (i.e. unpacking and packing). This would mean to add common code related to the federated authorisation solution to all the nodes. It is expected that it would not be very complex.
- Deal with the final authorisation option in the end nodes. As such, the node should identify, from the analysis of the SAML tokens included, which authorisation option is requested. Once identified, the transaction should fail in case of this authorisation option is not supported. If the option is supported, the node should launch the specific software component that actually implements the authorisation option. This would mean that this software component (i.e. authorisation reference implementation) has been previously distributed to the nodes that support the requested option.

7.3 Governance

As this solution is for a domain specific attribute in terms of eIDAS, the governance of the authorisation solution should be defined by the ISA/ISA^2 – CEF/eID and the eIDAS cooperation network.

First of all, the **governance of the domain expert group should be defined** between DIGIT, responsible for ISA/ISA^2 and CEF eID, and DGCNECT, business owner of CEF/eID. This definition of the governance should encompass the assignment of responsibilities, establishment of organisation and collaboration procedures. Furthermore the procedure for roll-out and delivery to the MS should be agreed.

Next, the proposed solution should be **submitted to the eIDAS Technical Sub-group**, to ensure that the solution is compatible with eIDAS. It is expected that the eIDAS Technical Sub-group could provide, on request, an advice regarding attribute schema design and a final review of the completed specification.

Then, the solution could be piloted after its approval by the eIDAS Technical Sub-group. This pilot would be oriented towards demonstrating that the chosen solution actually works with real applications.

Finally, the sustainability should be defined. The upcoming ISA² Action, "Semantic Interoperability for Representation Powers and Mandates", could be the most adequate initiative for assessing the sustainability.

8 Recommended solution

The envisaged federated authorisation solution should be designed on the basis of the assumptions identified in section 7.1.1 and fulfilling the requirements detailed in section 7.1.2. The solution should be sustainable, being based in current ECAS-STORK specifications and able to fit in eIDAS as EU-wide reference electronic identity framework. This is accomplished by the following **technical options**:

- **Authorisation attribute**. The option details and its major consequences are included in section 7.2.1 of this document.
- **Mandate attribute**. The option details and its major consequences are included in section 7.2.2 of this document.
- **Authorisation decision**. The option details and its major consequences are included in section 7.2.3 of this document.

As stated before, these options are **feasible**, have **reference implementations**, are **conformant with the SAML 2.0** standard, which is the core standard used at the STORK/eIDAS specifications, and have **benefits but also drawbacks**. The implications regarding STORK and eIDAS are as follows:

- The attribute based options (i.e. Authorisation and Mandate) require that the authorisation attribute is created as a new authorisation specific XML schema, following the eIDAS Technical Sub-group guidelines. This attribute should be exchanged through the eIDAS domain specific part. Finally, it is recommended that this new schema is maintained by an authorisation (or security) expert group supervised by the eIDAS Technical Sub-group.
- The Authorisation decision option requires that the eIDAS SAML and STORK 1.0-2.0 specifications should be changed to allow the exchange of AuthzDecisionStatement tokens.

Moreover, it should be noted that **these options are not mutually exclusive**. Therefore, the **most flexible solution is to allow all three options and each MS may choose** which solution wants to implement for the authorisation of public officials to access EC application. The solution could support seamlessly these three technical options, but the final technical option choice would depend on the MS and application specific needs.

In this way, **the solution is extensible because it could support not only cross-border but also cross-domain needs**. All options could be extended to a national level (e.g. a public official of a local administration requesting access to parts of national eGovernment portals), as well as to European cross-border level (e.g. a public official of one country accessing foreign eGovernment portals). Also, it could be extensible to the private sector (e.g. an employee of a foreign branch-office of a bank could use this solution to access corporate banking applications in the bank's home country, or citizens can use mandates to access on behalf of companies).

As a consequence of allowing three formats for transmitting authorisation information, the receiver of the authorisation will perform the interpretation of any format received. Within the scope of this study, this only affects the ECAS system. At first sight this seems complex, but probably the complexity doesn't increase significantly: in the end, the Authorisation attribute and the AuthzDecisionStatement hold a list

of <application>s, to which the user can access in <role>. Furthermore, any implementation other than ECAS could use the solution implemented by ECAS as a reference.

As discussed in 7.2.6, the mandate could also be used for natural persons representing legal persons, and from this mandate the authorisation to access applications could be derived. So the mandate could hold more generic powers of representation. These powers should be interpreted, until getting to <application>/<role> information. Once this interpretation is done, the result is the same as the Authorisation attribute and the AuthzDecisionStatement. This interpretation is complex, but doesn't affect the authorisation of public officials to access EC applications, so should be considered outside the scope of this study.

9 Conclusions and Recommended Next Steps

9.1 Conclusions

The first challenge of this study was to outline which projects and initiatives should be analysed in order to conduct a realistic and successful consolidation study on the federated authorisation. As a result, it was defined a methodological approach to accomplish this goal. The approach was based on the **methodological analysis of the Relevant Environment** and its influences on the envisaged federated authorisation solution.

The analysis conducted included not only extensive desk research on public documentation, but also very **fruitful discussions and meetings** with representatives of such Relevant Environment to ensure that the study considers the latest state of play. Their feedback and answers have been a very useful input for this study. The ISA 1.18 project team really appreciate and thank their collaboration and commitment.

The outcome of this study is the recommendation of a **federated authorisation solution** that indeed, **comprises three technical options that are not mutually exclusive and it could support not only cross-border but also cross-domain needs**. As required, the solution is sustainable, being based in current ECAS-STORK specifications and able to fit in eIDAS specifications as well. The technical options are the following: Authorisation attribute, Mandate attribute, and Authorisation decision.

These three technical options are based on the SAML 2.0 standard, have reference implementations and have been **contrasted with the ISA Action 1.18 stakeholders**. In this regard, it should be noted that, the **Mandate attribute option is the most sensitive one** because some concerns arisen during the study related to its legal feasibility and semantic suitability for authorisation purposes. **It is recommended that the legal and semantic concerns with the Mandate usage for authorisation purposes are tackled by the upcoming ISA² Action on mandates and powers**, "Semantic Interoperability for Representation Powers and Mandates", taking into account the significant work carried out on Mandates in STORK 2.0.

9.2 Recommended Next Steps

During this phase of Action 1.18 some points have been found which are candidates for future actions. These points are summarised in the following sections.

9.2.1 Integration of authorisation into the SEMIC Core Vocabularies

The recommendation would be to follow the approach of eIDAS that has **re-used the SEMIC Core Vocabularies**, Person and Business, to derive all the SAML attributes needed by the minimum eIDAS dataset and produce an eIDAS SAML Attribute Profile [8].

In line with this approach and the technical options proposed in this study, it is recommended to specify the Mandate as a SEMIC Core Vocabulary. It is expected that this standard Mandate would detail the tree of types of power until the authorisation to access an application is reached.

In order to reinforce such proposal, it should be noted that the MS have also requested the EC to proceed with a Mandate standardisation process because it is an important topic that currently is being managed and understood very differently at each MS. For this reason, a new ISA² Action is planned, "**Semantic Interoperability for Representation Powers and Mandates**", which will deal with the Mandate concept. This Action will deeply analyse its legal consequences, meaning and current barriers to adopt the mandates. The recommendation to that Action is to analyse the possibility that the Mandate also holds authorisation information and to tackle the concerns of its legal and semantic feasibility that have arisen during this study. An outcome of that Action, to promote the semantic interoperability, is to provide a common data model definition for such a concept in the form of **Core Mandate Vocabulary** that would be maintained by the SEMIC initiative. This would include all discussions with all EU Member States, in order to reach an agreement on its definition, usage and semantic meaning.

9.2.2 Integration of authorisation into the eIDAS specifications and software

Since the authorisation is a cross-cutting feature and would be needed by many applications, it is recommended that the authorisation concept should somehow be included in the specifications of eIDAS, which are maintained by the eIDAS expert groups. The reader should know what data is permitted but it should also be clear that the responsibility for this new element is not assumed by the eIDAS expert groups. So, probably, a reference in the eIDAS specifications to the organisation and document(s) which specify this new element could be a solution which satisfies both goals.

After this inclusion in the specifications, also a reference codebase should also be created accordingly in such a way that easy inclusion of this software into the eIDAS code base is guaranteed. For this code base the distribution mechanism should also be defined, as described in section 7.3.

9.2.3 Creation of an authorisation (or security) expert technical group

The attribute based options, Authorisation and Mandate, imply the creation of a new schema. It is recommended that this new schema is maintained and evolved by a domain expert group, (e.g. authorisation or security), that takes care of all the incoming needs, its long-term sustainability, and its eIDAS alignment. Nevertheless, joint collaboration will be established with the eIDAS Technical Sub-group in order to get their global sense feedback.

The establishment of such a domain expert group for this authorisation is described in section 7.3. As no such group exists for the moment, collaboration procedures will also need to be defined.

9.2.4 Decide on integration of authorisation into the STORK specifications and software

Depending on the complexity of integration, it may be recommendable to integrate the authorisation into the STORK common specifications and building blocks. Such integration will be carried out by the e-SENS project, which is responsible for the STORK maintenance until spring 2017.

Considering the required efforts for the AuthzDecisionStatement, such an investment in a platform which will disappear within a short time-frame is doubtful.

10 ANNEX I – History of Solutions in the context of ISA Action 1.18

This annex introduces some historical information about the evolution of the authentication and authorisation solutions in the context of ISA Action 1.18.

10.1 Original Authentication with ECAS

ECAS is the corporate authentication service of the European Commission, which enables web applications to authenticate centrally with, among others, a common strong password. When EC Applications use ECAS, the unauthenticated user is first redirected to ECAS where the user authenticates. Upon successful authentication, the user is redirected to the originating application along with a set of identity attributes which the application receives.

Initially, the user authenticated in ECAS, which provisioned the user's identity to the application. The application's administrator registered the access rights of the user in the application database, at the request of the foreign ministry. Normally there was one contact person for the application and several authorised users.

This is reflected in the following diagram.

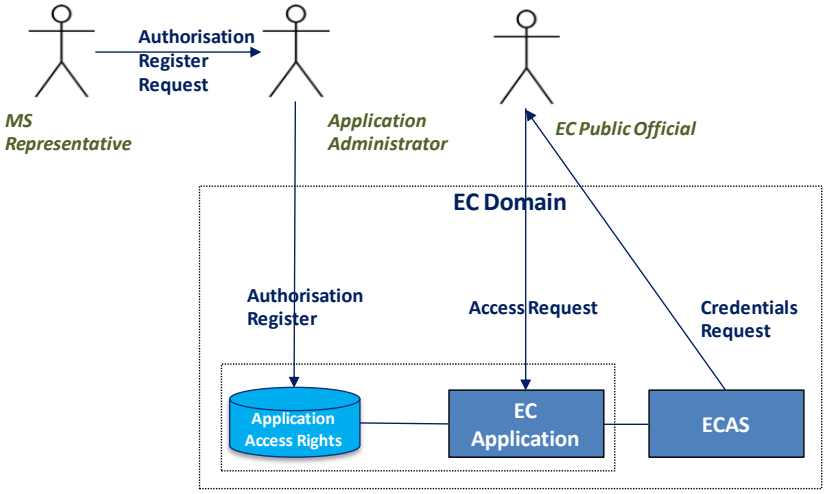


Figure 22: Authentication and authorisation process flows

10.2 ECAS Authentication with STORK

ECAS supports several authentication methods. Some years ago, ECAS connected to the STORK eID platform, allowing users to authenticate with their national credentials.

The ECAS-STORK integration needed to introduce a STORK eID component, hosted at the EC, which allowed formulating authentication requests to the STORK platform.

This extended architecture is shown in the following diagram.

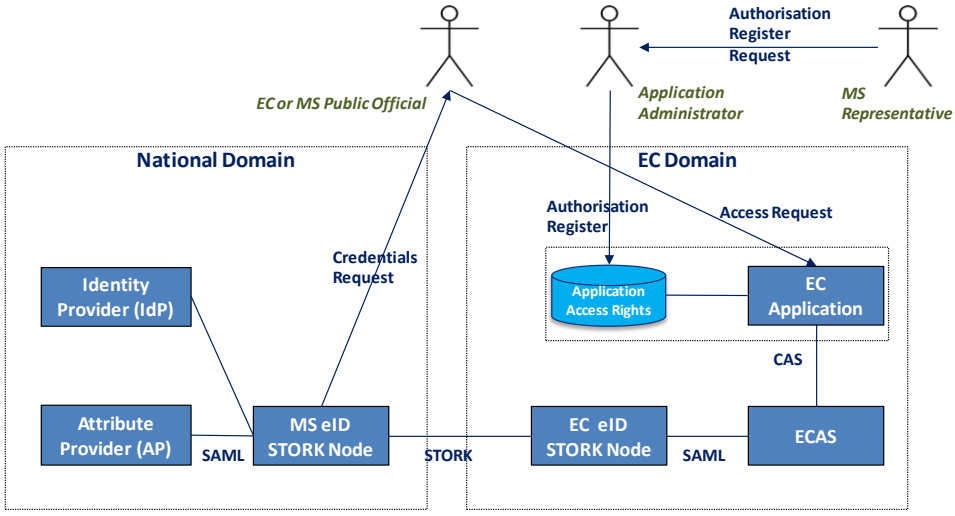


Figure 23: Authentication and authorisation process flows with STORK

If STORK is used for authentication, instead of requesting the user for his username and password, ECAS requests the user's data from the STORK node at the EC, which in turn forwards the request to the STORK node corresponding to the user's MS. After receiving the reply from the Identity Provider (IDP), the user is redirected the same way back. The access rights for each user are registered at the application, at the request of the MS representative. The application itself checks if the user is authorised to have access.

10.3 ECAS Authorisation with STORK (Previous Phase of ISA Action 1.18)

Prior to the current study, the Previous Phase of ISA Action 1.18 went one step forward and specified the process where the ECAS-STORK integration supported the exchange of authorisation information. This architecture specification was tested with a real EC application (CircABC) and a STORK eID node of one MS (Austria).

The solution was based on the exchange of additional attributes, which carried authorisation information, through the STORK eID platform. These new attributes were stored in the Attribute Provider (AP) of the MS, who was responsible for managing this information.

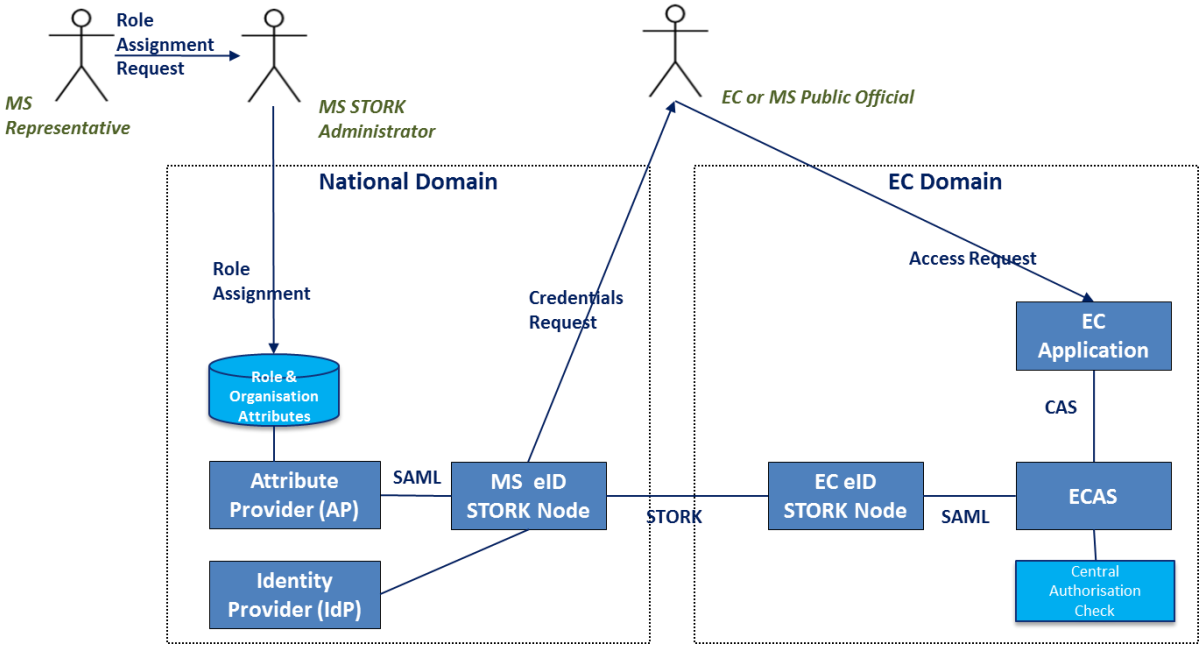


Figure 24: Authentication and authorisation process flows in Previous Phase of ISA Action 1.18

11 ANNEX II – Acronyms and Bibliographic References

11.1 Acronyms

Acronym	Description
AP	Attribute Provider
C-PEPS	Citizen PEPS
CED	Commission Enterprise Directory
CEF	Connecting Europe Facility
CIP	Competitiveness and Innovation Programme
DIGIT	Directorate General for Informatics
ebMS	OASIS ebXML Messaging Service
EC	European Commission
ECAS	European Commission Authentication Service
e-CODEX	e-Justice Communication via Online Data Exchange
eHGI	eHealth Governance Initiative
eID	Electronic Identity
EIF	European Interoperability Framework
EIS	European Information Systems
EO	Economic Operators
epSOS	European Patients Smart Open Services
e-SENS	electronic Simplified European Networked services
ETSI	European Telecommunications Standards Institute
EU	European Union
EUPL	European Union Public Licence
HCP	Health Care Professional
HCPO	Health Care Provider Organisation
IAM	Identity and Access Management
ICT	Information and Communications Technologies
IDP	Identity Provider
IHE	Integrating the Healthcare Enterprise

Acronym	Description
ISA	Interoperability Solutions for European Public Administrations
LDAP	Lightweight Directory Access Protocol
LSP	Large Scale Pilot
NCP	National Contact Point
NIF	National Interoperability Frameworks
OASIS	Advancing Open Standards for the Information Society
OSS	Open Source Software
PAP	Policy Administration Point
PBAC	Policy-Based Access Control
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PEPS	Pan-European Proxy Service
PIP	Policy Information Point
PSB	Project Steering Board
PSC	Point of Single Contact
QAA	Quality Authentication Assurance
REST	Representational State Transfer
S-PEPS	Service PEPS
SAML	Security Assertion Mark-up Language
SDO	Standard Development Organisation
SEMIC	SEMantic Interoperability Community
SPOCS	Simple Procedures Online for Cross- Border Services
SSO	Single Sign-On
sTESTA	secured Trans European Services for Telematics between Administrations
STORK	Secure idenTity across-borders linKed
TLS	Transport Layer Security
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

11.2 Bibliographic References

[1] ISA Action 1.18, "ISA 1.18 Home Page," [Online]. Available: https://joinup.ec.europa.eu/software/isa118/description. [Accessed June 2016].

[2] ISA, "ISA Home Page," [Online]. Available: http://ec.europa.eu/isa/. [Accessed June 2016].

[3] European Commission, "EUR-lex," 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN. [Accessed 2016].

[4] OASIS, "OASIS - SAML 2.0 specification," [Online]. Available: http://saml.xml.org/saml-specifications. [Accessed June 2016].

[5] OASIS, "OASIS XACML 3.0 specification," [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml. [Accessed June 2016].

[6] SEMIC, "SEMIC Home Page," [Online]. Available: https://joinup.ec.europa.eu/community/semic/description. [Accessed May 2016].

[7] SEMIC, "SEMIC Core Vocabularies," [Online]. Available: https://joinup.ec.europa.eu/community/semic/og_page/core-vocabularies. [Accessed May 2016].

[8] eIDAs Technical Sub-group, eIDAS SAML Attribute Profile, https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf, 2015.

[9] "STORK 2.0 Home Page," [Online]. Available: https://www.eid-stork2.eu/. [Accessed June 2016].

[10] e-SENS, "e-SENS Home Page," [Online]. Available: http://www.esens.eu/. [Accessed June 2016].

[11] European Commission, "Joinup portal," November 2015. [Online]. Available: https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10.

[12] SEMIC, "SEMIC Community of Practice data standards," [Online]. Available: https://joinup.ec.europa.eu/community/semic/og_page/cop-data-standards. [Accessed May 2016].

[13] SEMIC, SEMIC e-Government Core Vocabularies Handbook, https://joinup.ec.europa.eu/site/core_vocabularies/Core_Vocabularies_user_handbook/ISA%20Handbook%20for%20using%20Core%20Vocabularies.pdf, 2015.

[14] e. E. Group, Non-paper on minimum set of person identification data, 2014.

[15] e. E. Group, Non-paper on Minimum data set for legal persons and natural persons representing

legal persons, 2014.

[16] ISA², "ISA² Actions," [Online]. Available: http://ec.europa.eu/isa/library/documents/isa2-work-programme-2016-detailed-action-descriptions_en.pdf. [Accessed June 2016].

[17] OASIS, "SAML specifications," [Online]. Available: http://saml.xml.org/saml-specifications. [Accessed April 2016].

[18] OASIS, "SAML core," [Online]. Available: https://www.oasis-open.org/committees/download.php/35711/sstc-saml-core-errata-2.0-wd-06-diff.pdf. [Accessed 2016].

[19] OASIS, "OASIS Wiki pages," [Online]. Available: https://wiki.oasis-open.org/security/SAML21. [Accessed 11 April 2016].

[20] OASIS, "OASIS eXtensible Access Control Markup Language," [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html. [Accessed April 2016].

[21] OASIS, "OASIS SAML 2.0 profile for XACML," [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf. [Accessed May 2016].

[22] Kantara, "Kantara Initiative eGovernment Implementation Profile of SAML V2.0," [Online]. Available: http://kantarainitiative.org/confluence/download/attachments/38929505/kantara-report-egov-saml2-profile-2.0.pdf. [Accessed May 2016].

[23] Didier Ambroise, Anne-Laure Janeczek, Patrick Ruestchmann, Gil de Béjarry, epSOS D3.3.3 epSOS Interoperability Framework, http://www.epsos.eu/uploads/tx_epsosfileshare/D3.3.3_epSOS_Final_Interoperability_Framework_01.pdf, 2010.

[24] STORK WP4, "STORK 2.0 - D4.9 Final version of Functional Design," July 2015. [Online]. Available: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=66:d49-final-version-of-functional-design&Itemid=174&start=5. [Accessed April 2016].

[25] STORK WP4, "STORK 2.0 Final Version of Technical Specifications," September 2015. [Online]. Available: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174&start=5. [Accessed April 2016].

[26] STORK WP3, October 2015. [Online]. Available: https://www.eid-stork2.eu/index.php?option=com_processes&controller=document&view=document&task=streamFile&id=450&fid=2017. [Accessed April 2016].

[27] STORK 2.0 WP4, "STORK 2.0 - D4.11 Final version of Technical Specifications for the cross border

interface," August 2015. [Online]. Available: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174&start=5. [Accessed May 2016].

[28] eIDAS Expert Group, "Joinup - CEF eID," November 2015. [Online]. Available: https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10. [Accessed April 2016].

[29] eIDAS expert group, "eIDAS interoperability architecture," November 2015. [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/eidas_interoperability_architecture_v1.00.pdf. [Accessed April 2016].

[30] eSENS WP3, "D3.6 Scenario for governance models on short, medium and long-term," 2015. [Online]. Available: http://www.esens.eu/sites/default/files/e-SENS_D3.6_%282%29.pdf. [Accessed May 2016].

[31] e-SENS WP3, "D3.3 Report of integrated view of LSP sustainability strategies," 2014. [Online]. Available: http://www.esens.eu/sites/default/files/e-SENS_D3.3.pdf. [Accessed May 2016].

[32] epSOS, "epSOS Home Page," [Online]. Available: http://www.epsos.eu/. [Accessed May 2016].

[33] Martin Hurch, Gottfried Heider, epSOS D3.6.2 Final Identity Management Specification Definition, http://www.epsos.eu/uploads/tx_epsosfileshare/D3.6.2_Final_Identity_Management_Specificiation_Definition_01.pdf, 2010.

[34] epSOS, epSOS D3.7.2 FINAL SECURITY SERVICES SPECIFICATION DEFINITION - Section II Security Services, http://www.epsos.eu/uploads/tx_epsosfileshare/D3.7.2_SECTION_II_epSOS_Security_Services_01.pdf, 2010.

[35] ISA, European Interoperability Framework (EIF) for European public services, http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf, 2010.

[36] epSOS, epSOS D2.2.7 Final Recommendations, http://www.epsos.eu/uploads/tx_epsosfileshare/D2.2.7_Recommendations_v1.5.pdf, 2014.

[37] OpenNCP, "OpenNCP Home Page," [Online]. Available: https://openncp.atlassian.net/wiki/display/ncp/OpenNCP+Community+Home. [Accessed May 2016].

[38] EXPAND, "EXPAND," [Online]. Available: http://www.expandproject.eu/. [Accessed May 2016].

[39] SPOCS, "SPOCS Home Page," [Online]. Available: http://www.eu-spocs.eu/. [Accessed May 2016].

[40] SPOCS, “SPOCS Overview of Building Blocks,” [Online]. Available: http://www.eu-spocs-starterkit.eu/images/files/SPOCS_CM_June12_BB_v1_0_Final.pdf. [Accessed May 2016].

[41] STORK, “STORK - SPOCS collaboration,” [Online]. Available: https://www.eid-stork.eu/index.php?option=com_content&task=view&id=294&Itemid=69. [Accessed May 2016].

[42] SPOCS, “SPOCS Presentation,” [Online]. Available: http://www.eu-spocs.eu/index.php?option=com_processes&task=streamFile&id=21&fid=1302. [Accessed May 2016].

[43] Christian Schmitt, Michael Seeger, SPOCS D3.2 Specifications for interoperable access to eDelivery systems, Appendix 1 Security Architecture Development Process, http://www.eu-spocs-starterkit.eu/images/files/D3.2.1_Appendix1_SecurityArchitecture_Development%20Process.pdf, 2010.

[44] e-CODEX, “e-CODEX Home page,” [Online]. Available: http://www.e-codex.eu/. [Accessed May 2016].

[45] Giulio Borsari, Marco Velicogna, Albert Kappe, Alexander Weber, Liisa Nikkarinen, Zoi Kolitsi, Andreas Symeonidis, e-CODEX D7.3 High Level Architecture Definition, 2012.

[46] OASIS, “OASIS ebXML Messaging Service 3.0,” [Online]. Available: https://www.oasis-open.org/apps/org/workgroup/ebxml-msg/. [Accessed May 2016].

[47] H. Biersteker, F. Beukema, S. Wigard, E. Francesconi, e-CODEX D6.8 List of standards reusable assets and missing building blocks, http://www.e-codex.eu/news-and-media/media/deliverables.html?eID=dam_frontend_push&docID=805, 2013.

[48] Lesli Hommik, Viljar Tina, Adrian Klar, Rudi Teschner, Cyril Murie, Dea-Brix Hvillum, e-CODEX D4.7 eIdentity: Inventory and Requirements Documents, http://www.e-codex.eu/news-and-media/media/deliverables.html?eID=dam_frontend_push&docID=810, 2013.

[49] Adrian Klar, Rudi Teschner, Viljar Tina, Cyril Murie, Lesli Hommik, e-CODEX D4.8: Concept for Implementation of WP4, http://www.e-codex.eu/news-and-media/media/deliverables.html?eID=dam_frontend_push&docID=821, 2013.

[50] Giulio Borsari, Marco Velicogna, Remco Boersma, Zoi Kolitsi, Susanne Wigard, e-CODEX D7.1 Governance and Guidelines Definition, 2011.

[51] Marco Velicogna, Giampiero Lupo, Christine Lewis, Madalina Adam, Giulio Borsari, Francesco Contini, Gemma del Rey Almansa, Jose Matías González Bolivar, Zoi Kolitsi, George Pangalos, Yiannis Salmatzidis, Enrico Francesconi, Ernst Steigenga, Natalie Nickel, e-CODEX D7.4 Architectural Hands on Material, http://www.e-codex.eu/news-and-

media/media/deliverables.html?eID=dam_frontend_push&docID=806, 2015.

[52] e-CODEX, e-CODEX Catalogue of Interoperability Solutions, https://joinup.ec.europa.eu/catalogue/repository/e-codex-catalogue-interoperability-solutions, 2016.

[53] e-SENS, “e-SENS e-Delivery building block,” [Online]. Available: http://www.esens.eu/content/e-delivery. [Accessed May 2016].

[54] e-CODEX, “e-CODEX Roadmap on the sustainability of the e-CODEX project,” [Online]. Available: http://www.e-codex.eu/fileadmin/news/160212_Roadmap_e-CODEX_01.pdf. [Accessed May 2016].

[55] D. TAXUD, UUM&DS - UUM&DS System Architecture Document (UUM&DS-SAD), 2015.

[56] STORK 5.3, “Final report for pilot 3: eGovernment for business,” September 2015. [Online]. Available: https://www.eid-stork2.eu/index.php?option=com_processes&controller=document&view=document&task=streamFile&id=450&fid=2056. [Accessed April 2016].

[57] STORK Pilot 4, “Final report for pilot 4: eHealth,” October 2015. [Online]. Available: https://www.eid-stork2.eu/index.php?option=com_processes&controller=document&view=document&task=streamFile&id=450&fid=2051. [Accessed April 2016].

[58] eIDAS Technical Sub-group, “eIDAS SAML Message Format 1.0,” [Online]. Available: https://joinup.ec.europa.eu/sites/default/files/eidas_message_format_v1.0.pdf. [Accessed June 2016].

[59] e. T. Sub-group, eIDAS SAML Attribute Profile v1.0, https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf, 2015.

12 ANNEX III – Meetings

12.1 eSENS/eID adaptor development (NL representative)

Meeting Title:	eSENS/eID adaptor development meeting	**Meeting Date/Time:**	17-05-2016/11:00
Meeting Type:	Teleconference	**Meeting Location:**	Online
Meeting Coordinator:	Alice Vasilescu		

Attendee Name	Organisation
Alice Vasilescu	EC
Hans van der Burght	NL
John Heppe	everis
Marta Alberto	everis

12.2 eSENS/eID (MS representative - ES)

Meeting Title:	eSENS/eID	**Meeting Date/Time:**	25-05-2016/9:30
Meeting Type:	Teleconference	**Meeting Location:**	Online
Meeting Coordinator:	Alice Vasilescu		

Attendee Name	Organisation
Alice Vasilescu	
Carlos Gómez Muñoz	eSENS/eID ES
John Heppe	everis
Marta Alberto Monferrer	everis

12.3 SEMIC

Meeting Title:	SEMIC meeting	**Meeting Date/Time:**	25-05-2016/11:00
Meeting Type:	Teleconference	**Meeting Location:**	Online
Meeting Coordinator:	Alice Vasilescu		

Attendee Name	Organisation
Alice Vasilescu	EC
Miguel ALVAREZ RODRIGUEZ	EC – ISA
Athanasios KARALOPOULOS	SEMIC
John Heppe	everis
Marta Alberto Monferrer	everis
Joan Costa Sintes	everis

12.4 eIDAS dataset specification

Meeting Title:	eIDAS dataset – OASIS SAML	**Meeting Date/Time:**	27-05-2016/10:00
Meeting Type:	Teleconference	**Meeting Location:**	Online
Meeting Coordinator:	Alice Vasilescu		

Attendee Name	Organisation
Alice Vasilescu	EC
Adam Cooper	eIDAS dataset & OASIS SAML member
John Heppe	everis
Marta Alberto Monferrer	everis

12.5 e-SENS eID

Meeting Title:	e-SENS eID WP6	**Meeting Date/Time:**	09-06-2016/10:00
Meeting Type:	Mail	**Meeting Location:**	Online
Meeting Coordinator:	Alice Vasilescu		

Attendee Name	Organisation
Alice Vasilescu	EC
Klaus Vilstrup Pedersen	e-SENS eID WP6 (Manager)
Andrea Atzeni	e-SENS eID WP6 (member)
John Heppe	everis
Marta Alberto Monferrer	everis