SC112DI07171

D02.01 Report on the Architecture and Solution building blocks for e-Documents used in Member States

Report on Architecture and Solution Building Blocks for e-Documents used in Member States

Date: 11/05/2015

Document Metadata

Property	Value
Release date	2015-05-08
Status	Accepted
Version	2.01
Authors	Dusko Karaklajic – PwC EU Services Panagiotis Gouvas – Ubitech Monica Lopez Potes – PwC EU Services Zakaria Arrassi – PwC EU Services
Reviewed by	Susanne Wigard – European Commission Miguel Alvarez Rodriguez- European Commission Stijn Goedertier – PwC EU Services
Approved by	Susanne Wigard – European Commission

This report was prepared for the ISA Programme by:

PwC EU Services

Disclaimer:

The views expressed in this report are purely those of the authors and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Executive Summary

This report presents the result of the analysis of the solutions, architectures and standards related to electronic documents across three EU Member States (MS): Spain, Estonia and Denmark. The main objective of the report is to understand the usage of e-Documents by public administrations in MS and to identify Architecture Building Blocks (ABBs) and Solution Building Blocks (SBB) around e-Documents. The results of the analysis will serve as a basis for defining architecture template(s) that will solve specific needs/challenges related to usage of e-Documents by re-using the best practices identified in the analysed MS. The study was commissioned by the Interoperability Solutions for European public administrations (ISA) Programme of the European Commission, in the context of its Action 2.15 on e-Documents.

Based on the previous ISA study on e-Documents [1], we consider an e-Document any document in electronic format containing structured data and unstructured data used in the context of an administrative process. In other words, we treat an e-Document as an atomic information entity that plays a role in administrative processes across its entire lifecycle: from creation till archival and deletion. Also, the focus is on the *evidentiary* character of e-Documents in the processes they support. Our analysis will validate such a definition of e-Documents by comparing it with the definitions used in the analysed Member States.

This report is organized as follows: Chapters 1 and 2 introduce the study and the analysis framework followed to capture Solution and Architecture Building Blocks (SBBs and ABBs). Chapter 3 presents the main findings of the report, which are structured across the four levels of interoperability in the European Interoperability Framework (EIF): legal, organisational, semantic and technical interoperability. The ABBs and SBBs of the analysed e-Document solutions/standards are documented in Annex I.

Chapter 2 defines the analysis framework, which is inspired by the use cases “Document Interoperability Solutions” and “Compare Reference Architectures” of the European Interoperability Reference Architecture (EIRA)[1]. The analysis of each e-Document solution is structured as per EIRA view: legal, organisational, semantic and technical. The list below gives a preview of our research questions:

- **Legal view:** What are the legal drivers and the administrative requirements for usage of e-Documents? What are the requirements for their (legal) validity in administrative processes?
- **Organisational view:** How are e-Documents defined? What are the main processes that define their lifecycle (e.g. creation, storage, exchange, delegation, archival)? Who are the actors in these processes and how do they use e-Documents?

[1] EIRA: https://joinup.ec.europa.eu/asset/eia/asset_release/all

- **Semantic view:** What is the metadata associated with e-Documents? How are metadata sets defined? Which structures are used to bundle metadata, electronic signatures and content/payload together?

- **Technical view:** How is the authenticity of e-Documents achieved? How is the digital signing/validation of e-Documents implemented? Are there any other trust services used, e.g. time stamping? How is the access to and authentication of e-Documents implemented?

Chapter 3 formulates the main findings. They present different ways in which MS are solving the challenges related to using e-Documents and promote best practices.

"Electronic documents" vs. "Electronic records"

Before summarising the findings across the EIRA views, we try to reveal a possible cause of ambiguity around the term "**electronic document**" identified during the research. This ambiguity can potentially be caused by the translation and adaptation of the Moreq2 (Model Requirements for the Management of Electronic Records) [2]. The translations to national languages aim at adapting the MoReq2 terminology to the common language usage in the field, and the main difficulties are related to the terms **record** and **document**. MoReq2 defines a record as "**information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".** It is clear that a record is related to evidentiary and documentary character of information, which is in some other languages, e.g. Estonian, is denoted as a **document**. On the other hand, a document is not the same as a record; according to MoReq2, a document is **"Recorded information or object which can be treated as a unit".** Therefore, the translation and adaption of the terms **record and document** into the national languages possibly causes ambiguity in the terminology.

Independently of the used terminology, it is important to distinguish between the information with evidentiary and documentary character from any information object.

With regards to terminology, it is recommended to align to MoReq2 definitions- either by providing a clear mapping to the terminology in the national languages, or by using MoReq2 definitions when translating national standards to English.

With regards to other findings of this study, the most similarities between the analysed MS are found in the **legal view**. The usage of e-Documents in public administrations is commonly mandated by e-Government related laws and administration acts, which aim at increasing efficiency and performance, as well as at implementing so called a 'zero-paper policy'. Furthermore, the **legal constraints** for using e-Documents commonly originate from similar areas, which include public administration related laws, data protection and privacy legislation, and archiving regulations. For instance, the principle of **inclusion** mandates providing multi-channel access to electronic public services, which can imply support for both structured and unstructured (e.g. scanned paper documents) e-Document formats.

The analysis in the **organisational view** shows that all the analysed MS include the entire lifecycle of e-Documents into their national standards and architectures: creation, access, exchange, (long-term) preservation, and deletion/destruction. The specificities of these lifecycle stages are country-dependent and mainly influenced by the applicable legislation. The finding on the organizational view are further elaborated in Section 3.2.

The findings on the **semantic view** reveal differences in the logical organization of e-Documents. The Spanish approach explicitly defines the components of e-Documents: payload/content, metadata and electronic signature(s). In Estonia and Denmark, these definitions are influenced by e-Archiving laws, which stress the evidentiary character of electronic records and the necessity of their preservation. To solve the ambiguity, they define a logical model that explains relationships between information, document and record [3].

On the other hand, similar approaches for achieving interoperability on the level of metadata are identified. Both Estonia and Spain define a set of minimum required metadata to be associated with each e-Document used in public administration. By doing so, they enable the exchange of e-Documents between different administrative bodies, the use of documents and their archiving. In addition to the set of mandatory metadata, there is a set of optional metadata elements that can be used to fulfil specific needs of some administrative processes. Estonia considers the interoperability on the logical (i.e. logical organization of e-Documents) and metadata levels only a first step towards a complete interoperability, which includes the syntax level as well, e.g. XML schemas for e-Documents.

The **technical view** reveals multiple commonalities in SBBs found across MS. In particular, electronic signatures, seals and time stamps play a crucial role in the trusted use of e-Documents in administrative procedures. As a consequence, the central signing/sealing and validation platforms, which facilitate the establishment of a trust relationship between the parties are identified in all analysed MS. On the other hand, even though they all support the same technical standards (e.g. XAdES, CAdES and PAdES formats of electronic signatures and seals), the way multiple modalities of these formats are implemented can cause (cross-border) interoperability issues. We further elaborate on this topic in Section 3.4.

Finally, Annex I provides descriptions of the analysed solutions and architectures presented as sets of the EIRA ABBs and SBBs. Please note that the descriptions contain **only a partial analysis of** the solutions limited by the scope of this study and might not cover all the aspects of the specific solutions. For complete descriptions, we provide references to the corresponding documentation.

Annex I contains the following descriptions:

1. **The Spanish National Interoperability Framework (NIF)** [4], which is extended through a number of *Interoperability Agreements* [4]*,* including the ones for e-Documents and e-Files, authentic copies and e-Document management policies. Also a metadata schema has been developed and published. The NIF aims at establishing organisational, semantic and technical

interoperability in the electronic interactions with public administrations, as well as in the internal cooperation between public administrations. These agreements describe practical and operational aspects of interoperability for public administrations and citizens. Further, the descriptions from Spain include concrete e-Documents solutions developed in accordance with the National Interoperability Framework:

- **InSide,** a system for managing electronic documents and files so that they become compliant with the Spanish National Interoperability Framework (NIF);

- **@DOC,** which provides a horizontal services platform for management of e-Files and e-Documents. It enables client applications to incorporate most of the requirements of the NIF, as well as those for the exchange of recorded entries through the electronic registry.

Prior to the Spanish National Interoperability Framework (NIF), the specification SICRES 3.0 has been developed for the exchange of information between input/output registry offices. Annex I contains the description of GEISER, built in accordance with the SICRES 3.0 specification:

- **GEISER** (Integrated Registry Services Management), a comprehensive registry solution covering both management of the input/output registration offices as well as exchanging registries with the destination processing units.

SICRES specification is planned to evolve to provide a better integration with the NIF interoperability agreements for e-Documents. In any case, documentation has been developed in order to tackle SICRES 3.0 e-Documents according to NIF [5].

2. The **Estonian** multi-layer architecture for realisation of e-Document processes, including:

    - The Estonian implementation of the **MoReq2** (Modular Requirements for Records Systems) policy [3];

    - **Document Exchange Centre (DEC),** which connects distant ERMSs (Electronic Record Management Systems) of different local and government agencies for the secure transfer of records;

    - **DigiDoc**, a system for digital signing of e-Documents;

    - **x-Roads**, a service bus that links up various e-services and databases in the public and private sector.

3. The **Danish** standards for electronic file and document handling (FESD-II) and reference architecture for EDMS (Electronic Document Management Systems), as well as the cBrain F2 solution developed in accordance with the FESD-II standard, extensively used within Danish public administration.

Table 1: Glossary

Term / Acronym	Description
Architecture Building Block (ABB)	An abstract component that captures architecture requirements and that directs and guides the development of Solution Building Blocks (TOGAF [6]).
Attached Signature	Enveloped or enveloping signature (see below)
CAdES	Cryptographic Message Syntax Advanced Electronic Signature [7].
Common Electronic Registry	It enables the submission of applications, texts and communications to the **Spanish** General Administration and its public bodies which fail to conform to administrative procedures already covered by the electronic registers of the various authorities. For example, a document compliant with a regional electronic register may not be compliant with the requirements for the Spanish General Administration Registry. Thus, the Common Electronic Registry adapts the document to these specific needs.
Container	File holding data objects with related manifest, metadata and associated signature(s), under a specified hierarchy
CSV	In Spain, a Secure Verification Code (CSV) is an alphanumeric code linked to the public administration, body or entity and, where appropriate, to the person signing an electronic document, in any case allowing verification of the integrity of the document by accessing the corresponding electronic office.
Detached Signature	The signature is over content external to the signature element itself, and can be identified via a reference. Consequently, the signature is "detached" from the content it signs. This definition typically applies to separate data objects, but it also includes the instance where the signature and data object reside within the same XML document but are sibling elements [8].
DIR	DIR3 (Common Directory): The common directory provides a consolidated inventory common to the whole administration of functional units / public bodies, their offices and units associate economic management, budget - facilitating the maintenance and co-leader of information [9].
e-Document	Any document in electronic format containing structured data and possibly also unstructured data used in the context of an administrative process.
Electronic Register	The electronic registry is the place to submit requests, queries, applications forms and other official documentation linked to a public service within the administrative procedure. The submission is normally done via the electronic governmental website.
Electronic Seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. 'Creator of a seal' means a **legal person** who creates an electronic seal [10].
Electronic Signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign [10].

Enveloped Signature	The signature is over the XML content that contains the signature as an element. The content provides the root XML document element. Obviously, enveloped signatures must take care not to include their own value in the calculation of the signature value [8].
Enveloping Signature	The signature is over content found within an Object element of the signature itself. The Object (or its content) is identified via a reference) [8].
Input/output registry offices	In Spain, the input/output registry entities are administrative units mainly in charge of acknowledging all documents and notifications addressed to public administrations as well as the sending of documents, proofs of application forms and communications to citizens amongst others [11].
Legal Constraints	Other legal texts that the Interoperable European Systems need to comply with.
Legal Requirements	The legal text that mandates the creation of an Interoperable European System.
Metadata	Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information [12].
PAdES	PDF Advanced Electronic Signature [13]
Public Key Certificate (PKC)	Public key of a user, together with some other information, rendered unforgeable by electronic signature with the private key of the certification authority which issued it.
QR Code	A machine-readable code consisting of an array of black and white squares, typically used for storing URLs or other information for reading by the camera on a smartphone.
SIR	The System of Interconnection of Registers (SIR) is the basic infrastructure that enables the exchange of electronic input/output registries between public administrations in Spain [14].
Solution Architecture Template (SAT)	A Solution Architecture Template (SAT) is a subset of the Architecture Building Blocks of EIRA. It focuses on the most salient building blocks needed to build an interoperable solution addressing a particular interoperability need.
Solution Building Block (SBB)	A Solution Building Block can be defined as a concrete element that implements the required capabilities of one or more Architecture Building Blocks (TOGAF [6]).
Time Stamp	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Trusted List	In accordance with the e-Signature Directive [15] and eIDAS Regulation [16], each Member State establishes, maintains and publishes trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.
XAdES	XML Advanced Electronic Signature [17]

PREFACE- HOW TO READ THIS REPORT

This report is divided into two logical parts. The first one includes the executive summary, the introduction to the analysis and the main findings. It is meant to provide the reader with an overview of the usage of electronic documents in the analysed Members States, the identified challenges and the best practices to solve them. It is written to be understandable by the readers without deep technical knowledge in the field of electronic documents.

The second part of the report, in the annexes, contains the descriptions of the Solution Building Blocks (SBB) related to electronic documents identified in the analysed Member States. It contains technical details about the SBBs, and might require additional knowledge of the domain of electronic documents for proper understanding. The main purpose of this part is to provide the basis for the follow up of this report, which will be an architectural template for electronic documents inspired by the best practices identified in the Members States. On the other hand, each of the solution descriptions contains a short introduction meant to provide the reader with a brief overview of its main functionalities.

1 INTRODUCTION

This report contains the analysis of Architecture and Solution Building Blocks used in e-Document solutions in 3 EU Member States: Spain, Estonia and Denmark. The study is commissioned by the Interoperability Solutions for European public administrations Programme (ISA programme)[2] of the European Commission, in the context of its Action 2.15 on e-Documents and e-Files.

The findings of this report will serve as a starting point for building architecture template(s) which address specific needs related to the usage of e-Documents.

1.1 Context

As described by ISA Action 2.15, the "*administrative activity is distinguished by its documentary character, in the sense that the administrative documents are evidence of their activity and the external form of such act".*

In accordance with such description, this report focusses on the administrative activities in the MS and the evidentiary character of e-Documents in such activities. Consequently, in this study, e-Documents are considered to be *atomic* objects that participate in administrative processes. The definition of e-Document from a previous study is therefore adopted [1]:

> An e-Document is any document in electronic format containing structured data and unstructured data used in the context of an administrative process.

Despite the unified view of e-Documents as administrative objects, their logical and physical representation may differ. What exactly forms an e-Document from a logical perspective (e.g. descriptive metadata, content/payload, electronic signature, and the way these elements are bound together (e.g. container formats)) is a part of the analysis presented in this report.

1.2 Objectives

The main objectives of this study are to:

- Identify and document **architectures and solutions** dealing with electronic documents developed in the Member States and the main Architecture Building Blocks behind them;
- Identify the **reasons** behind the specific **architectural choices**, including drivers (legal or organisational) for the use e-Documents;
- Identify the challenges the MS are facing when using e-Document solutions, which include e.g. the legal validity of e-Documents or trusted use of e-Documents. These challenges will serve as the basis for building solution architecture templates, aiming to address them.

[2] ISA Programme, http://ec.europa.eu/isa/

1.3 Scope

This report targets the administrative processes that cover the entire lifecycle of e-Documents, from the moment they are created until they are archived or deleted. When selecting the MS for the analysis, the following selection criteria were taken into account:

- **The central character:** the existence of a central (national or regional) e-Document management policy or a solution architecture, which is used as a reference for multiple and actively used systems;
- **The cross-sectorial character**: the existence of cross-sectorial e-Documents solutions, preferably aligned to a common e-Document architecture;
- **The relevance to EU policies**, especially to the eIDAS Regulation [16] and its chapter about electronic documents.

1.4 Methodology

To achieve the objectives defined in Section1.2, the steps described below were followed:

- **Analyse and document** the identified e-Document solutions from the available materials via desktop research. In order to describe holistic e-Documents solutions and structure them coherently, we make use of the European Interoperability Reference Architecture v0.8.2 beta (EIRA)[3]. In particular, we make use of the EIRA *Document Interoperability Solutions* use case, which enables capturing the Architectural Building Blocks and Solution Building Blocks across four views: legal, organisational, semantic and technical. The analysis framework is explained in detail in Chapter 2 of this report.
- **Validate the results** with the architects of the analysed systems from the MS via virtual workshops;
- **Analyse the findings** and identify the reasoning behind the specific architectural decisions and needs related to the usage of e-Documents the MS might have.

[3] EIRA: https://joinup.ec.europa.eu/asset /eia/description

2 Analysis Framework

This chapter outlines the theoretical framework used to analyse the identified e-Documents solutions. Its purpose is to make sure that the analysis of e-Documents solutions is carried out in a consistent and harmonised manner, so that the findings can be aggregated in a meaningful and coherent way.

The analysis framework is inspired by the 'Document Interoperability Solutions' use case defined for the European Interoperability Reference Architecture (EIRA)[4] version 0.8.3 [18]. The analysis of each e-Document solution will be structured as per EIRA view: legal, organisational, semantic and technical. Each identified Solution Building Block will be mapped to a corresponding Architecture Building Block in the EIRA, enriched by additional information. This information can include a reasoning for using this particular building block, e.g. a specific EU policy, or a standard to which the SBB conforms.

In what follows, we list the questions used to discover and document the analysed solutions.

2.1 Description

Topic	Question	Applicable EIRA ABBs
Context	What is the domain that the service supports (e.g. Justice, Health)? Which stage of administrative process is supported by e-Documents (exchange, archival, e-Document management)?	N/A

2.2 Legal view

Topic	Question	Applicable EIRA ABBs
Legal Requirements	What are the legal requirements that mandates the usage of electronic documents? Are there any public policies on EU or national level that mandate usage of e-Documents? What are the main elements of the public policies that influence e-Document solution architectures?	Legal Requirements (Binding Instruments)
Legal Constraints	What are the main elements of the legislation that sets the constraints for e-Documents solutions?	Legal Constraints (Binding Instruments)

[4] EIRA: https://joinup.ec.europa.eu/asset /eia/description

Topic	Question	Applicable EIRA ABBs
Legal Validity	Is there any legal basis that defines requirements for the legal validity of e-Documents?	Legal Constraints/Legal Requirements

2.3 Organisational view

Topic	Question	Applicable EIRA ABBs
Public Service	What is the type of (public) service and/or administrative processes supported by e-Documents? Is it a front-end (user facing) or a back-end service?	Public Service/Service Delivery Model
Actors	Who are the actors involved in the public service? What are their roles in the identified public service?	User, Actors(European, National, Sub-national), Service Provider
e-Document Lifecycle	What are the main processes supported by the solution (e.g. exchange of e-Documents between the administrations, e-archiving)? Which stages in the e-Document lifecycle are included in those processes?	Business Process, Business Information Exchange, Business Transaction
Organisation	Is there any organisation-specific policy that the solution complies with (e.g. defining minimum security requirements for a validity and authenticity of e-Documents or data retention policy)? Which Solution Building Blocks (SBBs) are affected/introduced because of that policy?	Organisational Policy

2.4 Semantic view

This section outlines the semantic view of the analysis framework. The reader is referred to previous work on e-Document formats [1] and e-Document engineering [19] for further background and guidance on structured e-Document formats. Furthermore, the handbook on use Core Vocabularies [20] provides guidance on creating information exchange specifications extending a common core data model.

Topic	Question	Applicable EIRA ABBs

Security & Privacy	Is there a security and privacy policy in place and how is it implemented (e.g. which SBBs are affected by the policy)?	Security and Privacy Policy
Descriptive Metadata	What is the metadata associated with e-Documents? What is the purpose of that metadata (e.g. descriptive, process)? What are the applicable standards for metadata formats?	Metadata, Data Model
e-Document Representation[5]	How are e-Documents defined? Is the payload structured or unstructured? How are payload/content, descriptive metadata and signatures bundled together (e.g. containers)? What are the applicable standards?	Data Model

2.5 Technical view[6]

This section outlines the technical view of the analysis framework. Readers who are unfamiliar with the technical aspects of -Signatures are referred to corresponding ETSI Standards: XAdES [17], CAdES [7], and PAdES [13], which contain an introduction and the basic notations around electronic signatures.

Topic	Question	Applicable EIRA ABBs
Electronic Signatures/Seals	How are electronic signing/sealing and validation implemented? What are the applicable signature formats?	e-Signing/Validation service
Trust Services	Are there any time stamping functionalities used? What are the requirements behind them and where do they originate from? What are the applicable standards?	Trust management component/service
Long Term Preservation	Are there long term preservation signatures/seals used? Which archiving formats are used? What are the applicable technical standards?	e-Archiving component
Encryption	How is the encryption applied? What are the applicable technical standards? Which legislation/policy is directing the usage of encryption?	N/A

[5] We start from the assumption that the logical elements of e-documents are descriptive metadata, content/payload, electronic signatures and containers (See Glossary section).

[6] This includes Technical View-Application and Technical View-Infrastructure from EIRA [18]

Topic	Question	Applicable EIRA ABBs
Trust	In case of cross-administration or cross-border exchange, how is the trust relationship established across these domains?	Data exchange service/component, Trust management service/component

3 FINDINGS

This chapter presents a summary of the findings drawn by analysing and comparing the architectures and solutions from the analysed MS, structured according to four EIRA views.

3.1 Legal View

Legal requirements: The analysed use cases reveal that the mandate for the usage of e-Documents originates from the e-Government laws as well as administrative procedures laws. While Spain has a specific e-Government law [21], Denmark and Estonia set multiple legislations that deal with this subject, such as public information acts or archival laws. They mandate the enablement of the electronic interaction between the citizens and public administrations and require support for the electronic administrative processes and procedures. Being an integral part of these procedures, e-Documents support the initiatives of a "zero-paper" administration, as well as the increased efficiency and productivity.

E-Government laws are further provisioned through a number of standards and agreements, which will be elaborated in the organisational view of this report.

While the national legislations are driving the usage of electronic documents in administrative procedures to increase the efficiency, reduce costs and improve the citizen's experience, the traditional administrative procedures are set as a baseline. For instance, the legislation related to validity of electronically signed documents aim at equating them with the hand-signed ones. Instead of a simple transposition of the "paper" world to digital one, our recommendation would be to consider the additional benefits of digitization when defining public policies. For instance, electronic signatures and seals provide the ability of verification/validation of data integrity and authenticity which is not possible with handwritten signatures and stamps. Thus, electronic services can contribute to a higher level of authenticity of administrative documents.

Legal constraints: Independently from the context/domain of public services (e.g. health, tax), the following legal constraints influence the usage of e-Documents:

- Administrative procedure laws ([22], [23]), which establish general provisions for administrative procedures, and among others, the role of (electronic) documents and citizens' rights when interacting with public administrations;
- Electronic signature laws (Electronic signature directive [15] and corresponding national laws, as well as the new eIDAS Regulation [16]), which provide a framework for legal recognition of electronic signatures, seals and time stamps on e-Documents;
- Personal data protection laws, which set the conditions and liabilities for the processing of personal data;
- Archival related laws*,* which set the legal framework for archiving documents and files used by public administrations.

Legal validity of e-Documents: The requirements for considering e-Documents as valid evidentiary artefacts of administrative procedures originate from administrative procedure laws and aim at equating their status with the one of hand-signed documents. These are related to guaranteeing integrity and authenticity, which is achieved by applying electronic signatures, electronic seals and time-stamps. The following list describes the prominent use cases of these trust mechanisms in the administrative processes:

- **Electronic signatures/seals.** The only difference between signatures and seals is that the former are applied by natural persons, while the later are associated to legal entities. Both are used to ensure the following properties of e-Documents:
    - **Authenticity,** which guarantees that a document originate from the clamed entity;
    - **Integrity,** which guarantees that the content of a document is not modified by an unauthorized entity;
    - **Non-repudiation of origin,** which guarantees that a signer cannot deny that she/he has signed a document.

  For instance, a citizen uses his/her identity card to sign an e-Document before submitting it to a public administration. Similarly, a public administration (or a person authorized to act on its behalf) can sign or seal an e-Document before sending it to a citizen, or before forwarding it further to a different administration body.

- **Electronic time stamps,** which serve to prove that a data unit existed at a certain moment of time. They are usually implemented in combination with electronic signatures/seals. The prominent use cases of time stamps include the following:
    - Records the entrance of an e-Document into the system or vouches for the time when it enters a specific stage of an administrative procedure (e.g., a bid for a tender is submitted).
    - Periodic re-time stamping is used as one of the techniques to achieve long-term preservation of e-Documents and the accompanying electronic signatures or seals. They serve to preserve their validity despite the limited "life" of electronic certificates. This mechanism is elaborated in Section 3.4.

In addition to the necessity to sign/seal/time-stamp[7] e-Documents, there are requirements for the *quality* of these trust mechanisms. The assurance of this quality is achieved by requiring trust services to be provided by officially accredited entities (e.g. trust service providers listed in the national trusted lists[8]) or using the credentials (e.g.

[7] When mentioning the necessity to electronically sign/seal an e-document in the rest of this report, we always use the term "electronic signature". The strict differentiation between signature and seal will be clear from the context.

[8] Each Member State establishes, maintains and publishes trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified

a digital certificate) from the government issued identity documents. For more information about trust services in scope of e-Documents, refer to Section 3.4 of this report.

According the eIDAS Regulation [16], the legal validity of e-Documents should not be denied on the grounds that they are in an electronic format. The analysis of this study has revealed that there are different requirements for the legal validity of electronic documents among the Member States. Therefore, it is likely that national legislations will still play a role in defining precise requirements in this area. For instance, while all Estonian public authorities are obliged to accept digitally signed documents [24], Danish legislation still allows a few exceptions where the paper documents are required [25].

3.2 Organisational View

The findings in the organizational view are organized in accordance with the e-Document lifecycle, including creation, exchange, preservation and deletion of e-Documents.

Creation of e-Documents: An e-Document can originate from one of the following processes:

- Creation of a document in an electronic format, such as the submission through an electronic service (e.g. e-Government service). This also includes documents created by the citizen, e.g. MS Word, PDF or .txt documents;
- Digitisation of paper documents, which can be done either on citizen or government side.

In the analysed cases, a scanned paper document can become an official e-document either on the citizen side, where it is electronically signed by the citizen, or on the government side, where it is electronically sealed by a public administration body or signed on its behalf by a legitimate representative.

The main requirements related to the process of creating e-Documents are concerning the acceptable formats (structured and unstructured), the minimum set of metadata and the necessity to apply electronic signatures. In particular:

- The minimum set of metadata needs to be associated with each e-Document. This minimum set can be further extended depending on a specific use case, and it is subject of an agreement between the involved parties;
- The necessity of applying electronic signatures varies in the analysed MS. While Spain considers signatures (or seals) as an inherent part of official e-Documents, these are not mandatory in Estonia and Denmark. Therefore they might be absent if the legislation in scope does not require their presence;

trust services provided by them. The notion of trusted lists originates from the e-Signature Directive [15] and it is reinforced by the eIDAS Regulation [16].

- Both **structured and unstructured** content formats are supported, with a preference for structured ones whenever possible, in order to enable automated processing;
- The formats in which e-Documents are created depend on the specific process and its purpose, e.g. archiving. It is recommended to create e-Documents with long-term retention period in a format suitable for long term preservation, e.g. PDF/A.

To enable multi-channel access to government services and adhere to the **principle of inclusion**, public administrations often foresee to use both unstructured formats (e.g. scanned copies) and structured documents (e.g. via electronic forms) in the interactions with the public administrations.

While "digitally born" electronic documents clearly dominate in Estonia, a significant portion of Spanish citizens uses paper documents to interact with public administrations. To digitize these documents, the Spanish administration makes use of a specific solution, described in Section I.1.2 of this report.

Exchange of e-Documents: It is possible to notice a trend of unifying the way e-Documents are exchanged between public administration bodies in the analysed MS. While the Spanish public administrations use multiple solutions to do so due to Spain's decentralised government model, there is an effort to evolve to a more effective unified model. Similarly, Estonia already uses a multi-layered centralised model with its Document Exchange Centre (DEC) and x-Roads (see Section I.2.1) to provide document exchange facilities for its public administrations. Finally, in Denmark there is no centralized e-Document exchange system. However, according to the reference architecture of case and document handling systems there is a strict protocol (ODF/OOXML) regarding the format of the exchangeable 'object' which may be of diverse level of granularity.

The following commonalities between the analysed systems were noticed:

- A minimum set of exchange metadata is specified to ensure the basic interoperability between different public administrations;
- Beyond basic interoperability, these metadata are used for automated handling of the e-document;
- The exchange of e-Documents between public administrations is done via dedicated infrastructures (e.g. SARA network in Spain or DEC/x-Roads in Estonia). These networks aim at reliable and secure exchange of information;

Preservation of e-Documents:

The following commonalities related to the preservation of e-Documents were found:

- Retention policy: national e-Document architectures mandate the preservation of e-Documents for a certain period of time, but they do not specify the exact retention periods. Retention periods are primarily established on the basis of the requirements set forth in applicable legislation which, in certain circumstances, can also be obligatory for the private sector. It is up to a specific sector and the corresponding government bodies to set precise retention policies.

- Storage formats: general requirements around the storage formats aim at ensuring that the information can be transformed to different formats, so it can be used by other applications and/or transferred to the national archives. PDF/A format is usually recommended for the long-term preservation, but the other formats, such as PDF, XML, TXT and JPEG are "approved" as well.
- Security considerations: e-Documents should be preserved so that the required levels of confidentiality, integrity, availability are guaranteed. These levels are determined based on the criticality/sensitivity level of information contained the documents, which is typically indicated in the e-Document metadata.

To facilitate the transfer from the e-Document management systems to the archiving system, the Danish National Archives define a scheme that needs to be applied during the indexing of e-Documents.

Similarly, the Estonian Universal Archiving Module (UAM) facilitates the export of e-Documents to the National Archives. It also provides a possibility of converting the e-Documents into the formats suitable for long-term preservation, if needed.

Deletion/Destruction of e-Documents: Given their documentary and evidentiary value, the process of deleting e-Documents requires authorization from the competent authorities. In case of Estonia, the National Archive is in charge of apprising e-Documents in scope of the deletion process.

The Spanish National Interoperability Framework differentiates between the processes of deletion and destruction, where the later refers to physical destruction of the storage medium.

Furthermore, three deletion levels are defined based on the sensitivity of a document. The highest deletion level is applied to the most sensitive documents and should guarantee that the document cannot be recovered using any known techniques, including the advanced laboratory settings and utilities.

3.3 Semantic View

Logical modelling of e-Documents: The analysed systems consider an e-Document as an object that is part of an administrative process or transaction involving government bodies, citizens and businesses. Even though there is ambiguity around the exact notation used (e.g. e-Document versus electronic record), there is a common requirement about the evidentiary character of such administrative "objects".

From the logical perspective, e-Documents consist of the content/payload (structured or unstructured), electronic signatures and metadata around it. The Spanish National

Interoperability Framework lists exactly these three logical elements as inherent parts of an e-Document [26]. The Danish model defines a notion of a logical document, which can contain a number of sub-elements (denoted as "attachments" in the cBrain F2 implementation). Both logical documents and its sub-elements can have a set of metadata and electronic signatures associated with them. Finally, Estonia defines a file format conformant to ETSI standards (BDOC file format [27]) to bundle the payload, metadata and electronic signatures into an atomic structure.

Apart from the agreement on a common logical representation of e-Documents, the analysed MS aim at two other aspects of semantic interoperability:

- Interoperability on the level of descriptive metadata, which enables the basic automated processing of e-Documents and their re-usability and exchange between different bodies. This is achieved by defining a mandatory set of minimum metadata for e-Documents. The minimum set of metadata can be further extended to meet the requirements of specific use-cases.
- Interoperability on the level of the e-Document format, i.e. semantic/syntax interoperability. In case of Estonia, this is set as a long-term goal which will fully automate the processing of e-Documents. The reader is referred to a study on e-Document formats [1] and e-Document engineering methods [19] carried out in the context of the ISA programme.

Logical grouping of e-Documents: The way multiple e-Documents are bundled together is addressed in different ways. It is determined in a "bottom up" approach, to address the specific use cases within national public administrations. Spain defines the concept of e-Files, which consist of references to e-Documents (indexes), their signature and the metadata (Section I.1.1.3). On the other hand, Estonia relies on a container format for embedding source data and signatures, denoted as a "BDOC file format", aligned with the XAdES Baseline Profile [17] and the AsiC container format [28]. Finally, in Denmark, according to the e-Document schema defined by the Document Management and Case Handling Reference Architecture, an e-Document can contain references to other e-Documents. In addition, e-Documents can be further grouped into "cases", to support the specific needs of public administrations.

Descriptive Metadata: Estonia, Spain and Denmark take a similar approach to ensure a minimum interoperability between different administrative bodies; thus they define a set of mandatory metadata that need to be associated with each e-Document. Similarly, these countries define a set of optional metadata, depending on the specific purpose (e.g. digital archiving) and which can be subject to an agreement between parties involved in an administrative process. Such an approach also enables the automated processing of e-Documents to a certain extent.

It could be argued that these metadata can be classified in the following categories

- Functional metadata (interpreted by the e-Document exchange endpoints);
- Regulatory metadata (refer to regulatory requirements);
- Classification metadata;

- Process-related metadata (relate to workflows).

All these metadata categories may apply to different levels of granularity i.e. e-Document and e-File.

Representation of e-Documents: The way the payload/content, the metadata and the signatures are put together is addressed in different ways.

Estonia solves these problems by defining the base standards, including:

- A subset of XAdES elements and parameters (addressed as "BDOC profile of XAdES") [27];
- Requirement profiles for PKI, time-stamping and certificate validation services and corresponding XAdES building blocks;
- A container format for embedding source data and signatures (addressed as "BDOC file format");
- In order to perform the aforementioned definitions, the XAdES Baseline Profile [17], the AsiC format and its Baseline Profile are used [28].

On the other hand, Spain supports the following five different modalities for binding e-Document content, metadata and signatures.

- CSV code;
- XAdES detached;
- XAdES enveloped;
- CAdES detached;
- CAdES attached;
- PAdES.

For some information on the XML schemas of the signatures above, please refer to Annex I.1.5.

In Denmark there is a specific format used for electronic signature; namely the OCES format. OCES is the Danish abbreviation for Public Certificates for Electronic Services ("Offentlig Certifikat for Elektronisk Services"). Launched in 2003, OCES comprises Public defined certificate policies from the Danish National IT and Telecom Agency, a CA approved by the agency and the underlying PKI.

3.4 Technical View

Electronic signing/validation: Technical interoperability for electronic signatures is achieved via mandatory usage of standard electronic signature formats, based on XAdES, PAdES and CAdES formats, as explained above.

A so-called "circle of trust" is created by relying on national trusted lists under national supervision. Each Member State establishes, maintains and publishes trusted lists which include information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them, as mandated by eIDAS regulation [16]. The reliance on national trusted lists facilitates creation and validation of cross-border trust relationships.

All analysed countries facilitate the usage of electronic signatures and seals by providing a common platform and client applications for electronic signing and validations (e.g. Spanish @Firma, Estonian DigiDoc, OpenSigner in Denmark). These platforms also serve as a "trust anchor" by providing support for multiple PKI Validation Authorities.

Electronic seals: The concept of electronic seal is similar to the concept of electronic signature, with a difference that a creator of a seal is a legal person. According to the eIDAS Regulation [16] an electronic seal "*should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.*" Further, the regulation allows for an authorised representative of a legal person to use his/her qualified electronic signature instead of the respective qualified electronic seal.

An interesting usage of electronic seals is identified within GEISER, an e-Document solution in Spain (see Annex I.1.2). They are used to provide a legal validity of an "authentic copy" to the scanned documents provided by the citizens in the paper format to the public administrations.

The validity of an automated application of electronic seals, i.e. without the direct involvement of a natural person is not particularly defined by the eIDAS Regulation. If it is not addressed through a secondary legislation, it is likely that it will be subject to national regulations.

Time stamping: Time stamping is considered an important trust service across the e-Document lifecycle. Its purpose is twofold:

- To record when an e-Document enters a system or a specific lifecycle stage or a stage in the administrative procedure (e.g. submitted);
- To certify the validity of an electronic signature (algorithm, key length) at a given date.

Further, time stamping, along with the long-term electronic signature formats, is used to achieve long term preservation of e-Documents. In combination with electronic signature profiles (e.g. XadES-A [17] by ETSI), re-time stamping is used to validate and time-stamp a document using the updated electronic signature (algorithm and key length), thus protecting the signed content from vulnerabilities of outdated algorithms.

Time stamps play an important role across the e-Document lifecycle as they provide reliable evidence of the timeline of an administrative process and protect signed e-Documents against outdated signature algorithms.

Encryption: The analysed systems consider encryption as an optional functionality, which is typically provided on the transport level. The communication between public administrations is done either via a dedicated national (e.g. SARA network in Spain) or international (e.g., sTESTA) network, which provides encryption capabilities at the transport-level. On the other hand, the Estonian CDOC file format (an extension used to distinguish encrypted files) [29] leaves the possibility for encryption on the document level (XML or other binary) by providing an encryption/decryption key exchange infrastructure for the involved parties.

The personalized encryption relies in most of the times to asymmetric encryption algorithms. Practically, this means that a sender uses the public key of the receiver in order to encrypt the payload. This means that transferable object resides in a governmental cloud until it is claimed by the receiver. If the receiver does not claim it or its key-pair is lost the transferable object is useless. Because it is practically impossible to recover encrypted (and signed) documents when the private key is lost, it is proposed (as a best practice) to include the sender as a default-receiver as well, in addition to the actual recipients.

Verification Code: In addition to the validation of authenticity of e-Documents achieved through dedicated signature/seal validation tools (e.g. @Firma in Spain, DigiDoc in Estonia and OpenSigner In Denmark), there are additional mechanisms that can serve this purpose.

An indicative mechanism relies on the usage of a verification code that is generated based on the electronically signed document (through a hashing technique) and may be delivered to various stakeholders (citizens, civil servants) through many communication channels (email, printed stamp). Based on an online verification service any stakeholder can verify the authenticity of a signed document or even retrieve it. In most of the times, this code is hard to remember or to manually copy to the respective verification portal-form; thus some complementary techniques that aim to increase the level of automation are employed. Such a technique is the QR-embedding technique according to which the verification code per se and the verification URL are encoded in QR format. In this way any QR reader (practically any smart phone) can be used to retrieve the code.

An example of such a mechanism in Spain is the Secure Verification Code (CSV) - an electronic fingerprint of an e-Document mainly used in the Spanish administration. It can be considered a trust management component for e-Documents and e-Files. The CSV is an alphanumeric code that appears on all electronic documents issued electronically, either as an alphanumeric string or as a bar code. Its main purpose is to ensure authenticity of printed copies of e-Documents.

> The Secure Verification Code (CSV) plays an important role in allowing the unique identification of e-Documents across their entire lifecycle including both paper and electronic representations.

4 CONCLUSION

The goal of this study was to understand how the selected Members States are using electronic documents across their lifecycle and to identify Architecture and Solution Building Blocks that can be used to define e-Document related solution architecture templates.

The study reveals a number of findings on how the analysed Members States are solving the challenges related to the usage of e-Documents across legal, organizational, semantic and technical views. It is noticed that the three analysed Member States have the common drivers for using e-Documents: increased efficiency of the administrative procedures, improved citizen’s experience and reduced costs. To achieve these objectives, they define national architectures and standards that cover entire lifecycle of e-Documents, from creation till archival and destruction.

The analysed Member States are facing a number of common challenges when dealing with e-Documents, such as defining the requirements for their legal validity, standardised usage of trust services (electronic signatures, seals and time stamps), or “unified” logical models for e-Documents and e-Files. The ways in which these challenges are being solved are country-specific. It can be noticed that the countries’ governmental structures (e.g. centralised or decentralised) affect the approach to e-Documents. For instance, the Spanish NIF and its interoperability agreements for electronic documents provide common specifications for e-Documents, e-Files and metadata, in accordance to which the specific solutions can be built. Due to the decentralised nature of the Spanish government model, there are different solutions and systems dealing with e-Documents and e-Files responding to the necessity to provide solutions addressing the specific needs of each government/body/entity. On the contrary, Estonia follows a multi-layered centralised approach (DEC, DigiDoc, x-Roads), which provides a single solution for dealing with e-Documents in public administrations.

Also, it is noticed that the analysed MS are trying eliminate the usage of paper in the interaction with the citizens either through digitization of paper documents, or by replacing the paper forms through the usage of web portals. For the “back-end” processing of electronic documents by the public administrations, the focus is put on increased productivity and efficiency, e.g. through the structured storage formats, easy retrieval, and simplified/transparent workflows, e.g., cBRAIN F2 solution from Denmark.

Overall, this study identified the common points and differences in solving e-Document related challenges across the analysed Member States across legal, organisational, semantic and technical views. These will serve as a starting point for defining architecture templates for e-Documents, where the identified standards and best practices will be taken into account.

5 REFERENCES

[1] "Analysis of Structured E-Documents in Trans-European Systems," [Online]. Available: http://ec.europa.eu/isa/documents/misc/analysis-of-structured-e-document-formats-used-in-trans-european-systems_en.pdf.

[2] "Moreq," [Online]. Available: http://ec.europa.eu/idabc/en/document/2303/5644.html.

[3] "MoReq in Estonia," [Online]. Available: https://www.mkm.ee/sites/default/files/estonian_et_-_chapter_0_english.pdf.

[4] "National Interoperability Framework (Spain)," 2010. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/pae_Esquema_Nacional_de_Interoperabilidad/ENI_INTEROPERABILITY_ENGLISH_3.pdf.

[5] "Government of Spain "Application Guide for the Technical Interoperabiity Standard of the Data Model for the exchange of input/output registries in SICRES 3.0"," [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/Normas_tecnicas/Guia_de_Aplicacion_NTI_Asientos_Registrales_SICRES3/2013_ENI_GuiaAplicacion_NTI_SICRES_3_0__2_edicion_NIPO_630-13-095-X.pdf.

[6] The Open Goup, "The Open Group Architecture Framework (TOGAF®)," 2011. [Online]. Available: http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html.

[7] "CAdES," [Online]. Available: http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.08.03_60/ts_101733v010803p.pdf.

[8] "XML DSIG," [Online]. Available: http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/.

[9] "DIR- Spain," [Online]. Available: http://administracionelectronica.gob.es/ctt/dir3.

[10] European Union, "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, OJ L 257, 28.8.2014, p. 73–114," 2014. [Online]. Available:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[11] "Government of Spain "Royal Decree 772/1999, of May 7, by which the submission of applications, documents and communications addressed to the General Administration, the issuing of copies of documents and return of originals and the regime of registry off"," 1999. [Online]. Available: http://www.boe.es/buscar/act.php?id=BOE-A-1999-11499.

[12] "Understanding Metadata," [Online]. Available: http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

[13] "PDF Advanced Electronic Signature Profiles;," [Online]. Available: http://www.etsi.org/deliver/etsi_ts%5C102700_102799%5C10277804%5C01.01.02_60%5Cts_10277804v010102p.pdf.

[14] "Government of Spain "Technical Interoperability Standard for SICRES 3.0"," 2011. [Online]. Available: http://administracionelectronica.gob.es/ctt/sicres.

[15] "eSig. Directive," 1999. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093.

[16] "REGULATION (EU) No 910/2014," [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

[17] "XML Advanced Electronic Signatures (XAdES)," [Online]. Available: http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.01_60/ts_101903v010401p.pdf.

[18] European Commission, ISA Programme, "European Interoperablity Reference Architecture (EIRA)," 2014. [Online]. Available: https://joinup.ec.europa.eu/asset/eia/description.

[19] "Guidelines for public administrations on e-Document engineering methods," 2014. [Online]. Available: https://joinup.ec.europa.eu/node/93213.

[20] European Commission, ISA Programme, "Handbook for using the Core Vocabuarlies," 2014. [Online]. Available: https://joinup.ec.europa.eu/webdav/core_vocabularies/www/Core_Vocabularies_user_handbook/.

[21] "Government of Spain, "Law 11/2007, of 22 June, on electronic access to Public Services for citizens"," 2007. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/pae_NORMATIVA_ESTATAL_Leyes/LAW_11-2007_22Jun2007_eGov_Spain_NIPO_000-10-075-0.pdf.

[22] “Law No. 30/1992 of November 26, 1992 on General Government and the Common Administrative Procedure,” [Online]. Available: http://www.boe.es/buscar/act.php?id=BOE-A-1992-26318.

[23] “Estonian Administrative Procedure Act, consolidated text 1 January 2012,” 2012. [Online]. Available: https://www.riigiteataja.ee/akt/123022011008?leiaKehtiv.

[24] “Estonian Digital Signature Act [Online],” [Online]. Available: http://www.legaltext.ee/text/en/X30081K4.htm.

[25] “iDABC Denmark,” [Online]. Available: http://ec.europa.eu/idabc/servlets/Doc4083.pdf?id=32340.

[26] “Government of Spain, “Technical Interoperability Standard for E-Documents”,” 2011. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/LEGISLACION_2011_13169_traduccion_al_ingles_NTI_for_E-documents--1-/Electronic%20Document%20Interoperability%20Standard%20NIF%20Spain.pdf.

[27] “BDOC FIle Format,” [Online]. Available: http://www.id.ee/?id=34336.

[28] “Asic Container,” [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.01.01_60/ts_102918v010101p.pdf.

[29] “CDOC File Format,” [Online]. Available: http://www.id.ee/?id=35780#cdoc.

[30] “Government of Spain, “Technical Interoperability Standard for the Catalogue of Standards”,” 2012. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/LEGISLACION_2012_BOE-A-2012-13501_Catalogue_of_standards_ENI_publicacion_oficial_2012/Catalogue%20of%20Standards%20NIF%20Spain.pdf.

[31] “Spanish eSig Policy,” [Online]. Available: http://administracionelectronica.gob.es/ctt/politicafirma#.VPmGNfnF8s5.

[32] “CMIS Standard,” [Online]. Available: http://docs.oasis-open.org/cmis/CMIS/v1.1/os/CMIS-v1.1-os.html.

[33] “InSide Specifications,” 2013. [Online]. Available: http://administracionelectronica.gob.es/ctt/resources/Soluciones/323/Area%20descargas/Especificaciones-InSide-1-1.pdf?idIniciativa=323&idElemento=492.

[34] “Government of Spain, “Technical Interoperability Standard for E-Files”,” 2011. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/LEGISLACION_2011_13170_traduccion_al_ingles_TIS_for_E-files/Electronic%20File%20Interoperability%20Standard%20NIF%20Spain.pdf.pdf.

[35] “Government of Spain, “Technical Interoperability Standard for E-Document Authentic Copy and Conversion Procedures”,” 2011. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/LEGISLACION_2011_13172_trad_ingles_TIS_for_E-document_authentic_copy_and_conversion_procedures/Authentic%20Copies%20And%20Conversion%20Intero.

[36] “Government of Spain "Technical Interoperability Standard for Digitisation of Documents",” [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/LEGISLACION_2011_13168_traduccion_al_ingles_TIS_for_Document_Digitalisation/Digitisation%20of%20Documents%20Interoperability%20Standard%20NIF.

[37] “Government of Spain, “Technical Interoperability Standard for the Spanish Public Administration E-Signature and Certificate Policy”,” 2011. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/LEGISLACION_2011_13171_traduccion_al_ingles_TIS_for_the_Spanish_Public_Administration_E-Signature_and_certificate_policy/eSignature%20Policy%.

[38] “Government of Spain "Facturae formats",” [Online]. Available: http://www.facturae.gob.es/formato/Paginas/version-3-2.aspx.

[39] “Government of Spain "@Doc platform description",” [Online]. Available: http://administracionelectronica.gob.es/ctt/resources/Soluciones/371/descargas/Descripcion de la Plataforma -Doc.pdf?idIniciativa=371&idElemento=987.

[40] “ STORK Web Site [Online],” [Online]. Available: https://www.eid-stork.eu.

[41] “Estonian Public Information Act [Online],” [Online]. Available: https://www.riigiteataja.ee/ert/act.jsp?id=13256729.

[42] “Estonian Identity Document Act [Online],” [Online]. Available: https://www.riigiteataja.ee/en/eli/504112013003/consolide.

[43] “The Estonian ID Card and Digital Signature Concept Principles and Solutions, AS Sertifitseerimiskeskus (www.sk.ee) 2003,” [Online].

[44] “Estonian Personal Data Protection Act [Online],” [Online]. Available: https://www.riigiteataja.ee/en/eli/512112013011/consolide.

[45] “Estonian National Archives Act [Online],” [Online]. Available: https://www.riigiteataja.ee/en/eli/ee/526092014003/consolide/current.

[46] “Estonia State Secrets And Classified Information Of Foreign States Act [Online],” [Online]. Available: https://www.riigiteataja.ee/akt/108072011049.

[47] “Estonian Population Register Act [Online],” [Online]. Available: https://www.riigiteataja.ee/en/eli/516012014003/consolide.

[48] “Estonian Government of the Republic Resolution on the Data Exchange Layer of Information Systems [Online],” [Online]. Available: https://www.riigiteataja.ee/akt/119012011015.

[49] “OpenSigner Reference,” [Online]. Available: http://www.openoces.org/opensign/references/.

[50] “Record Management Metadata-Estonia,” [Online]. Available: https://www.mkm.ee/sites/default/files/dokumendihalduse_metaandmed.pdf.

[51] “DigiDoc Component [Online],” [Online]. Available: https://e-estonia.com/component/digidoc/ .

[52] “X-ROAD system [Online],” [Online]. Available: https://www.ria.ee/x-road/.

[53] “X-ROAD Service Protocol [Online],” [Online]. Available: http://x-road.ee/docs/eng/x-road_service_protocol.pdf.

[54] “X-ROAD Regulation [Online],” [Online]. Available: http://ftp.ria.ee/pub/x-tee/doc/X-Road_regulations.pdf.

[55] “Danish e-Government Strategy,” [Online]. Available: http://www.digst.dk/Servicemenu/English/Policy-and-Strategy/eGOV-strategy.

[56] "FESD I Standard," [Online]. Available: http://www.digst.dk/Arkitektur-og-standarder/Standardisering/Datastandardisering/Sag-og-dokumentomraadet/FESD-standarderne/FESD-standarderne-i-seneste-version/FESD-Udvekslingspakke.aspx.

[57] "FESD II Standard," [Online]. Available: http://www.digst.dk/Arkitektur-og-standarder/Standardisering/Datastandardisering/Sag-og-dokumentomraadet/Faelles-offentlig-ESDH-kravsspecifikation.

[58] "Danish Open Standards," [Online]. Available: http://www.digst.dk/Servicemenu/English/IT-Architecture-and-Standards/Open-standards.

[59] "CBRAIN Corporate Site," [Online]. Available: http://www.cbrain.com/.

[60] "Danish Administration Act," [Online]. Available: http://www.wipo.int/wipolex/en/details.jsp?id=1089.

[61] "Danish Archive Act," [Online]. Available: https://www.sa.dk/media(3000,1033)/Danish_Archives_Act.pdf.

[62] "Danish Data Protection Act," [Online]. Available: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/.

[63] "Danish Act on Digital Signatures," [Online]. Available: http://www.steadlands.com/data/legislation/denmark.pdf.

[64] "Danish e-Document Structure," [Online]. Available: https://digitaliser.dk/pages/ResourceView.aspx?ResourceView=444163.

[65] "Danish e-Document XSD format," [Online]. Available: https://digitaliser.dk/pages/ResourceView.aspx?ResourceView=514979.

[66] "Danish NETID reference," [Online]. Available: http://www.nets.eu/dk-da/Produkter/Sikkerhed/Documents/Nets_produktark_NemID_tjenesteudbyder_EN.pdf.

[67] "Danish NetID Interoperability Guide," [Online]. Available: http://www.nets.eu/dk-da/Service/kundeservice/nemid-tu/NemID-tjenesteudbyderpakken-okt-2014/Documents/NemID%20Integration%20-%20OCES%20%28Implementation%20Guidelines%20for%20NemID%29.pdf.

[68] “EC 45/2001,” 2001. [Online]. Available: http://www.iss.europa.eu/fileadmin/euiss/documents/Data_protection_documents/Regulation_45_2001.pdf.

[69] “Government of Spain, “Royal Decree 4/2010, of January 8th, which regulates the National Interoperability Framework within the e-government scope”,” 2010. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/pae_Esquema_Nacional_de_Interoperabilidad/ENI_INTEROPERABILITY_ENGLISH_3.pdf.

[70] “Government of Spain, “Royal Decree 3/2010, of January 8th, which regulates the National Security Framework within the e-government scope”,” 2010. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad/ENS_SECURITY_ENGLISH_final_2_.pdf.

[71] “ Resolution of the Secretary of State for Public Administration of 28 June 2012, giving approval to the Technical Interoperability Standard for E-Document Management Policies,” 2012. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/pae_NORMATIVA_ESTATAL_Otras_disposiciones_relevantes/2012-10048_E-document-management-policies_NIF_Spain_NIPO-630-12-210-X.pdf.

[72] “Government of Spain "",” [Online]. Available: http://administracionelectronica.gob.es/ctt/politicafirma#.VO3hwWOGd8E.

[73] “Government of Spain "Resolution of 29 November 2012 of the Ministry of Public Administration by which the Agreement approval of the Policy on Electronic Signature and Spanish General Administration Certificates is published. ",” 2012. [Online]. Available: http://administracionelectronica.gob.es/ctt/politicafirma#.VO3hwWOGd8E.

[74] “PAdES,” [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf.

[75] “Government of Spain, “Technical Interoperability Standard for E-Document Management Policies”,” 2014. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/e_Document_Management_Policies_Interoperability_Standard_NIF_Spain/e-Document%20Management%20Policies%20Interoperability%20Standard%20NIF%20S.

[76] “Government of Spain, "e-Signature Policy",” 2011. [Online]. Available: http://administracionelectronica.gob.es/ctt/politicafirma.

Annex I e-DOCUMENTS SOLUTIONS IN THE MEMBER STATES

Annex I contains the following descriptions:

1. **The Spanish National Interoperability Framework (NIF)** [4], which aims at establishing organisational, semantic and technical interoperability in the electronic interactions with public administrations, as well as in the internal cooperation between public administrations. This annex also includes descriptions of concrete e-Documents solutions developed in accordance to the National Interoperability Framework: GEISER, InSide and @DOC;

2. The **Estonian** multi-layer architecture for realization of e-Document processes, including the Estonian implementation of **MoReq2** [3], **Document Exchange Centre (DEC)**, **DigiDoc**, a solution for digital signing of e-Documents, and **x-Roads**;

3. The **Danish** standard for electronic file and document handling (FESD-II), including cBrain F2 solution as the reference implementation, and the reference architecture for EDMS (Electronic Document Management Systems).

I.1 Spain

This annex provides an overview of the Spanish approach to the implementation of eGovernment measures. The main purpose of these measures is to provide the right of communicating with and within the public administration by electronic means. This annex is focused on the use of e-documents and e-files as a measure to provide interoperability and an electronic means to tackle information either from the citizen or other public administrations. According to this, the sections below will detail:

- The national interoperability framework and related interoperability agreements for managing e-files and e-documents.
- The analysis of specific solutions implemented as a consequence of the legal framework created around the enabling of electronic access and interoperability. The solutions considered are:
  - GEISER
  - InSide
  - @Doc

The following chart describes how these solutions interact within the Administrative procedure:

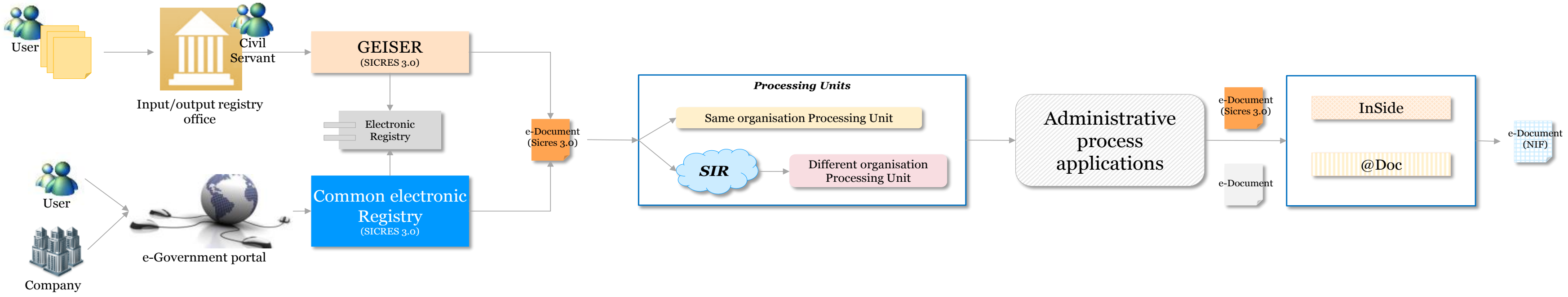


Figure 1: Spanish e-Document solutions overview

GEISER is the application to manage and register (among other functionalities) in the Electronic Registry[9] all the documents submitted in the input/output registry offices. These documents are submitted by citizens on a paper. GEISER registers the entry and creates an e-Document compliant with SICRES 3.0 specification.

The Common electronic Registry enables the submission of applications and other documents conforming or not conforming to the administrative procedures. The submission of documents and documentation is carried out through electronic forms that generate an e-Document compliant with SICRES 3.0 specification. The electronic submission of information is mandatory for legal persons and optional for natural persons.

Due to the fact that the presence of paper in the relationship with public administration is still of high relevance, the study is focusing on GEISER.

Once the e-Document is created, it is sent to the processing unit addressee of the document. If the destination is a different organisation from which the e-Document has been created, the latter will be redirected through SIR. SIR is the System that allows the interconnection of registers enabling the exchange of electronic recordings from input/output registries between public administrations.

When the e-Document reaches the correct unit/organisation, this is processed using the proprietary business/administrative process applications such as Tax management, request management or registration as a different kind of entity (e.g. from Limited Society to Anonymous Society). These applications are independent from the solutions explained in this document, and the integration (if any) has to be built "ad hoc".

Finally, InSide and @Doc share functionalities regarding the management of e-Documents. Both applications are meant to generate e-Documents compliant with the National Interoperability Framework specification. Therefore, the input is normally an existing document (on electronic means) on which the minimum required metadata and e-Signature requirements are to be included and the specific format is to be applied.

Currently, there are two specifications for e-Documents in Spain that respond to different needs: SICRES 3.0 for the exchange of information between input/output registry entities and the National Interoperability Framework with a wider scope. There is not an explicit relationship between both standards, but an evolution of both schemas of data to establish a more direct correspondence is planned.

The solutions explained in this document are compliant with the specifications mentioned as follows:

Solution	Specification
GEISER	SICRES 3.0
InSide	National Interoperability Framework (NIF)

[9] The electronic registry is the place to submit requests, queries, applications forms and other official documentation linked to a public service within the administrative procedure. The submission is normally done via the electronic governmental website.

Solution	Specification
@Doc	National Interoperability Framework (NIF)

I.1.1 Interoperability agreements for e-Documents and e-Files

This section provides an overview of the Spanish interoperability specifications for e-Documents implemented in various e-Document solutions such as GEISER, InSide, and @Doc.

I.1.1.1 Introduction

The Spanish National Government has developed a legal eGovernment framework aiming at achieving organisational, semantic and technical interoperability in the electronic interactions with public administrations, as well as in the cooperation between public administrations. The National Interoperability Framework (NIF) has been developed through *Royal Decree 4/2010,* and extended through a number of *Interoperability Agreements* [4]*.* These agreements describe practical and operational aspects of interoperability of public administrations and citizens.

According to law "11/2007, of 22 June, on electronic access to Public Services for members of the public", an e-Document is defined as "**Information of any type in electronic format and saved on an electronic media in accordance with determined format and which is susceptible to identification and processing***"* [21]*.*

The e-Documents that are used in administrative processes can be found in two different ways:

- As administrative documents; and
- As other e-Documents that could become part of an e-File.

Both as isolated documents or being part of an e-File, e-Documents have to comply with the **Interoperability agreements for e-Documents** [26]. This standard is applicable to the Federal Government, defined as the General State Administration, the Administration of the Autonomous Communities and the entities that make up the Local Administration, including the public law entities (entities that carry out their activity according to the public law) linked or dependent on them.

Additionally to the interoperability agreements for e-Documents previously referred to, there is a technical standard of an interoperability data model for the exchange of information between input/output registry entities[10]. This standard is based on the

[10] The input/output registry entities are administrative units mainly in charge of acknowledging all documents and notifications addressed to Public Administrations as well as the sending of documents, proofs of application forms and communications to citizens amongst others [11].

specification SICRES 3.0[11] [14] (in Spanish), whose approval by the competent corporate bodies was conducted prior to the development of NIF for e-Documents.

Given that both standards maintain an implicit relationship due to the fact that electronic documents can be transmitted between registry entities, a functional link between them is necessary until there is an evolution of schemas of data to establish a more direct correspondence. However, this evolution has not yet been accomplished.

Therefore and given that the SICRES 3.0 specification has a limited scope, the Spanish Interoperability Agreements related to e-Documents and e-Files are described in what follows through the EIRA ABBs and SBBs, as explained in Chapter 2.

I.1.1.2 Legal view

Spain has developed a legal framework for e-Government that provides support for the interoperability among public administrations and for the interactions with citizens. It aims at:

- The evolution of public services to digital ones;
- The evolution to a "zero-paper" administration;
- The increase in the efficiency in the performance of administrative procedures.

Figure 2 shows the EIRA legal view of the Spanish NIF.

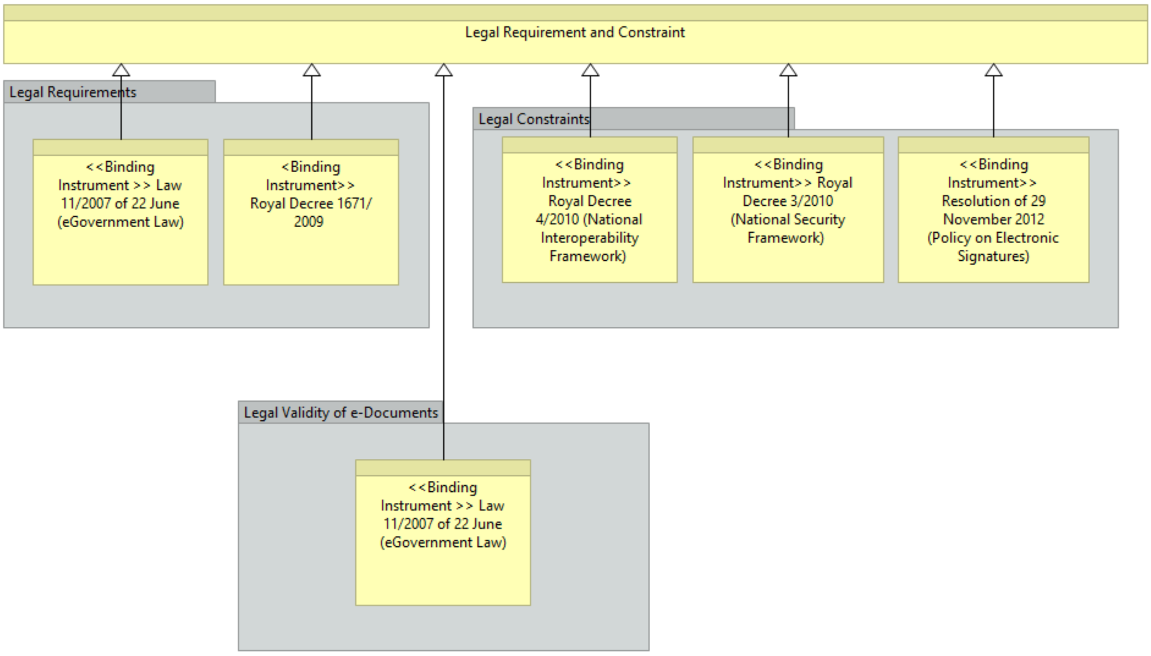
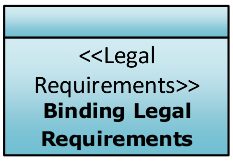

Legal Requirement and Constraint
Legal Requirements
<<Binding Instrument >> Law 11/2007 of 22 June (eGovernment Law)
<Binding Instrument>> Royal Decree 1671/ 2009
Legal Constraints
<<Binding Instrument>> Royal Decree 4/2010 (National Interoperability Framework)
<<Binding Instrument>> Royal Decree 3/2010 (National Security Framework)
<<Binding Instrument>> Resolution of 29 November 2012 (Policy on Electronic Signatures)
Legal Validity of e-Documents
<<Binding Instrument >> Law 11/2007 of 22 June (eGovernment Law)

Figure 2 Legal View of the Spanish NIF

[11] SICRES 3.0: It standardises and establishes a unique way, global and comprehensive data model for the exchange of information between registry entities regardless of the registry system origin or destination, and technology exchange.

It is important to point out that the Legal Validity of e-Documents is explained as a separate group due to the fact that is of special relevance within the context of this study. This is because of the need to deal with official and valid documents within the Administrative Procedure. Otherwise, and in terms of the present EIRA version, it would be a legal constraint.

ABB Legal Requirements



SBB: Binding Legal Requirements

Legal references considered in the development and implementation of e-Documents are:

- **Law 11/2007 of 22 June** (eGovernment Law), among others, introducing the obligations to provide citizens with electronic access to public services, the notion of electronic administrative process, electronic document and e-Archive. This law settles the basis for the creation of the National Interoperability Framework according to which the Interoperability agreements have been developed and all the needs around e-Documents and e-Files.

  This law establishes electronic communication with public administration as a *right* for the general public (as one of the available channels to establish the relationship with the public administration) while it is an *obligation* for public administrations.

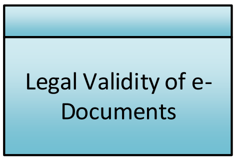
- Royal Decree 1671/2009 of November 6, which partially develops the Law 11/2007 of 22 June on electronic access of citizens to public services.

ABB Legal Constraints

SBB: Binding Legal Constraints

- Royal Decree 4/2010 of 8 January the Ministry of the Presidency by which the **National Interoperability Framework** (NIF) is regulated. Once the National Interoperability Framework had been formalised via this Royal Decree, it had to be capitalised on by the implementation of different solutions (amongst which GEISER and InSide, here described, have been implemented).

- Royal Decree 3/2010 of 8 January that governs the **National Security Framework** (NSF). It defines the information security policy and sets the basic principles and minimum requirements for the adequate protection of information.
- Resolution of 28 June 2012 the Secretary General of the Ministry of public administrations by which the Technical Standard for Interoperability for electronic documents Management Policy is approved.
- Resolution of 29 November 2012 of the Ministry of public administration by which the Agreement approval of the Policy on Electronic Signature and Spanish General Administration Certificates is published.
- Application Guide of the Technical Standard for Interoperability of the Policy Management of Electronic Documents.



Specialisation: Legal Validity of e-Documents

According to Law 11/2007 of 22 June on electronic access to Public Services for members of the public:

- public administration bodies may validly issue by electronic media the administrative documents (the ones referred to in article 46 of Law 30/1992, on the Legal Regime of the public administration and Common Administrative procedures), providing that they contain one or more electronic signatures.
- Administrative documents should contain electronic time references (time stamping) that should be provided by electronic services when the nature of the document requires it.
- The providers of electronic services for time stamping should be specified by State public administration.

More specifically and concerning the electronic copies created in the registry offices, the following criteria are to be followed in order to consider the e-Document legally valid. According to Article 44 of the Royal Decree 1671/2009 (development of Law 11/2007), when electronic images are created by the public administration, they will have the nature of authentic electronic copies, with the scope and effects detailed in Article 46 of Law 30/1992 of 26 November, provided that the following conditions are met:

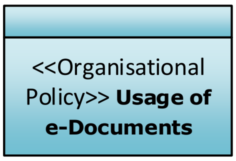
- The copied document is an original or an authentic certified copy.
- The electronic copy is authorized by electronic signature using the systems detailed in Articles 18 and 19 of Law 11/2007 of 22 June.
- The electronic images are encoded according to any of the formats and levels of quality and technical conditions specified in the National Interoperability Framework.

- The electronic copy should include the information that characterises the document as a copy. Therefore, it will be mandatory to fill the correspondent metadata.

- The copy should be obtained according to the rules of responsibility (governance) and procedure approved in each case, including automated granting.

I.1.1.3 Organisational view

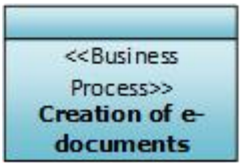
ABB- Organisational Policy



SBB: Usage of e-Documents in administrative processes

Description: Each Spanish public administration defines and decides on the usage of e-Documents in the different services driven by the underlying Administrative Procedure. Once this is decided, the public administration will establish 1) the list of such services and the conditions to use them, 2) data, 3) documents and 4) records in electronic format that will be available for the rest of the administrations.

In these conditions, administrations will specify the aims, modalities of consumption, interaction and general requirements that potential users must satisfy as well as the criteria to access the services, government mechanisms of the interoperability systems and the security conditions.



SBB: Creation of e-Documents

- **Sources:**
  - **Electronic**, by which the document has been initially created in an electronic format. This is the case when the citizen interacts with public administration services via e-Administration portals such as tax declaration or application forms for different types of requests.

    In case the public administration is creating an e-Document, the e-Document originates from the administrative procedure applications that create a document in electronic format. In order to ensure compatibility with NIF standards, specific solutions (such as InSide or @Doc) have to be used in order to provide the main characteristics (metadata, signature) an e-Document should have.

  - **Paper,** by which in order to create an electronic document, it will be necessary to include a digital image that shows the contents and layouts of the original document. Additionally, complementary metadata can be assigned during the digitisation process in order to meet specific description requirements.

- **Formats and Standards:**
  - The standards allowed for the creation of e-Documents are those specified in the Technical Interoperability Standard for the catalogue of Standards.
  - The format to be chosen for the creation of the e-Document should take into account and be handled according to the purpose each format in the standard has been established for.
  - Other formats can be used when specific characteristics or requirements are needed or when they are required to preserve a document as an e-evidence of activities or procedures (in case of format conversion).
- **Processes:**
  - **The digitisation process** should be done through electronic procedures.
  - **Generation of authentic copies:** The copies generated via this process will have the same legal value as the original document since they have to be identical to the original electronic documents, with no changes in format or content. Authentic copies are created under the following requirements:
    - They should be new e-Documents containing the full or partial content of the original document they are a copy of.
    - In order to consider the copy an authentic one, it has to be signed using one of the signature systems allowed.
    - Metadata information has to be specified.
  - **Conversion:**
    - This involves the creation of a new e-Document that will have a different format or version from the original one.
    - The main difference in the specification regarding conversion of e-Documents is the need for preservation of the content, context and structure of the original document and the identification of the components that require special treatment during the conversion.
    - Should the conversion need further certification as an e-copy the requirements on the metadata set for the generation of e-copies should be also met.

SBB: Exchange of e-Documents

Description: The exchange consists in sending the e-Documents with the components and structure previously defined, without the need for considering the type of the application or other structures involved in the exchange.

Other structures can be used to exchange e-Documents between public administration agencies if the parties have previously agreed on the structure.

However, if the exchange is going to take place with third parties (different public entities) involved, it has to be done according to the XML Schema for e-Document exchange defined in **XML Schemas in Spain**.

Requirements:

- The exchange of e-Documents among different public administrations is preferably done using SARA network (SBB: SARA Network).
- If a document is a part of a registry entry, it shall be treated as an attachment to the exchange data message.
- In case of the exchange involves the transfer of permanent document management responsibilities, the transferor should check the document's authenticity and integrity at the moment when the exchange takes place.
- From any transfer a certificate of the actions performed should remain in the sender file, either by metadata traceability or by any other method considered appropriate.
- The transfer of e-Files will be carried out sending in first place the e-Index and later each of the e-Documents contained. This transfer will be done one by one and following the order/distribution established in the index.

SBB: Access to e-Documents

Description: The access to the e-Documents is provided by public administration Agencies or Bodies at their e-offices or through the enabled communication channels. These entities should allow:

- Showing the e-Document contents in compliance with the regulation on formats.
- The basic information on each of the e-signatures.

- A description of the minimum required metadata and the values assigned to them.

Requirements: The access to e-Documents and e-Files is determined by the protection measures established in the National Security Framework, more specifically by:

- Personal Data
- Data Rating

SBB: Preservation of e-Documents

Methods:

- Document-by-document.
- Compiling information contained in data bases. In this case, it will be necessary to have the correct criteria for reconstructing the electronic forms or applications used to create documents.

Requirements:

- The documents should be stored by electronic media ensuring the authenticity and integrity of the information required to reproduce the document.
- Transferring data to other formats and media should be considered, in order to guarantee that the information can be accessed from different applications.
- Security measures in the storing process: the media or format in which documents are stored should guarantee the integrity, authenticity, confidentiality, quality, traceability, protection and conservation of the documents. Amongst these measures:
  - Backups
  - Data Protection measures
  - Data support system protection
  - Personal Data protection
- Regarding **e-Archiving** (when necessary), each government entity will determine the minimum periods for archiving e-Documents depending on the administrative procedures.

SBB: Destruction or Deletion of e-Documents

Description: The removal of a set of electronic documents can be the result of a series of circumstances, among which the following can be found:

- By an elimination agreement.
- By reformatting.
- For failure of storage media and its replacement.
- For file transfer.
- By changing storage medium for obsolescence or migration between systems.

Requirements: The elimination of administrative documents will require authorization from the competent authority and subsequent communication to the rating authority.

Processes:

- **Deleting Level 0:** Removal of documents using standard operating system commands. This procedure provides no guarantee against unauthorized disclosure of information.
- **Deleting Level 1:** Removal of data or sensitive documents from a storage medium to ensure the data cannot be reconstructed using normal system functions or file recovery programs. The data may still be recoverable, but this would require special laboratory techniques or advanced utilities.
- **Deleting Level 2:** Removal of data or sensitive documents from a storage device in order that the data cannot be reconstructed using any of the known techniques.
- **Destruction:** The storage medium is physically destroyed, preventing its use.

ABB-Actors

SBB: e-Documents actors

Description: Two different actors can be found in the dealing with e-Documents in the public administration:

- Citizens in their dealings with the government.
- Governments and public administrations and the existing relationships between them.

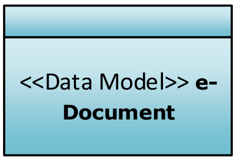
Concerning the governmental actors the main ones that took part in the definition of the Interoperability Agreements and are the ones to implement and use e-Document solutions are the following:

- Tax Agency
- Social Security

- General Directorate of Traffic
- State Archives

I.1.1.4 Semantic view

ABB-Data Model



SBB: e-Document

Description: According to the Technical Interoperability Standard, the main components of the e-Documents are the following:

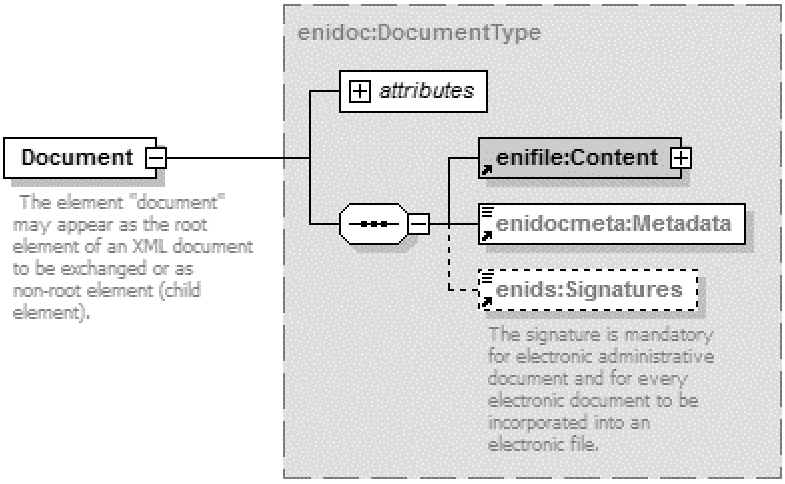

enidoc:DocumentType
attributes
Document
The element "document" may appear as the root element of an XML document to be exchanged or as non-root element (child element).
enifile:Content
enidocmeta:Metadata
enids:Signatures
The signature is mandatory for electronic administrative document and for every electronic document to be incorporated into an electronic file.

Figure 3: e-Document components

- **Contents:** Understood as the document data or information contained in it. This information should be compliant with the standards defined in the **Technical Interoperability Standard for Standard Catalogues** [30], among which the following can be found:
  - **Text:** Comma separated values, HTML, XHTML, CSS, XML, PDF, PDF/A, RTF, TXT, SVG, MHTML.
  - **Image:** JPEG, PNG, TIFF.
  - **Sound:** MP3, MPEG-1, OGG-Vorbis.
  - **Video:** MPEG-4, WebM.

  The content of the e-Document is structured according to the following schema:

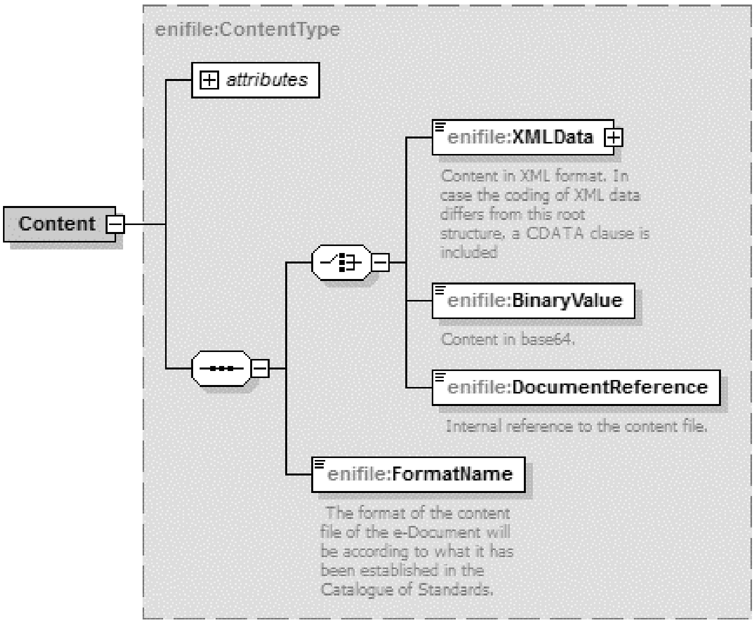

enifile:ContentType
attributes
Content
enifile:XMLData
Content in XML format. In case the coding of XML data differs from this root structure, a CDATA clause is included
enifile:BinaryValue
Content in base64.
enifile:DocumentReference
Internal reference to the content file.
enifile:FormatName
The format of the content file of the e-Document will be according to what it has been established in the Catalogue of Standards.

Figure 4: e-Document content components

- **e-Signature:** All e-Documents will have at least one e-Signature attached (according to the Resolution of 29 November 2012 of the Ministry of public administration by which the Agreement approval of the Policy on Electronic Signature and Spanish General Administration Certificates is published).

  According to the NIF, the e-document is encoded to provide an integrated, secure and multichannel accessibility. The standards used to encode the document are specified in the Technical Standard for Standard Catalogues, mentioned below. Amongst these standards Base16, Base32, Base64, UCS and UTF can be used.

- **Metadata:** e-Documents' metadata provide the minimum information required to identify the document such as its origin (source), legal validity and purpose, amongst others (the minimum metadata required for the creation of e-Documents can be found in The technical Interoperability Standards for e-Documents). Further requirements regarding e-Document metadata is addressed in the semantic view, more specifically in the SBB: e-Document Metadata.

<<Data Model>> **e-File**

SBB: e-File

An electronic file is a dossier, saved on an electronic media, which contains electronic documents organised either in folders, in sub-files or as independent documents.

Description: According to the Technical Interoperability Standard, the main components of e-Files are the following:

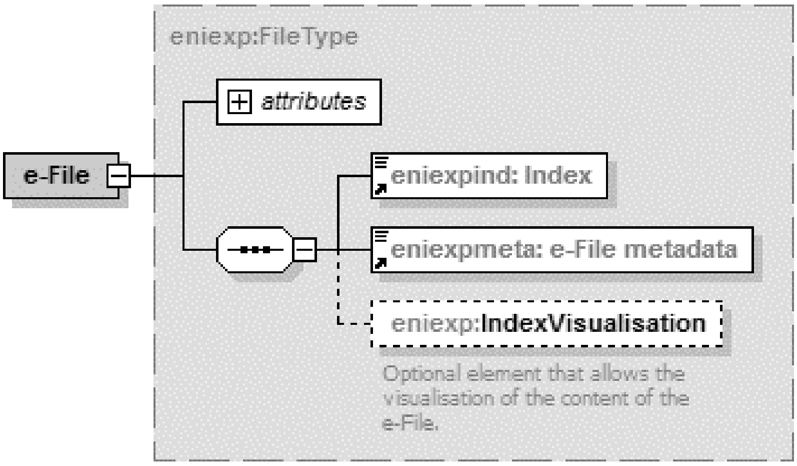

eniexp:FileType
attributes
e-File
eniexpind: Index
eniexpmeta: e-File metadata
eniexp:IndexVisualisation
Optional element that allows the visualisation of the content of the e-File.

Figure 5: e-File components

- **e-Documents:** These documents should comply with the structure and format specifications in the Technical Interoperability Standard for e-Documents. e-Documents can be included in e-Files following different structures:
  - As independent elements.
  - In folders; a set of e-Documents created for functional purposes for which there are not general specifications.
  - As a part of a sub e-File; a nested e-File that follows the structure defined in the Technical Interoperability Standard for e-Files.
- **e-Indexes:** They should guarantee the integrity of e-files and their retrieval whenever necessary (according to the provision in Article 32.2 of Law 11/2007 of 22 June). e-Indexes should contain the whole set of e-Documents associated with a file at a given moment, and if necessary, their distribution in folders or files. The main purpose of the e-Indexes is the organisation and help in the visualisation of the e-Documents and folders contained in the e-File. More specifically the content of the index is the following:
  - Creation date of the electronic index.

- For each element the index is pointing at:
- e-Documents:
  - Document identifier
  - Hash
  - Algorithm used to create the hash
  - Date of inclusion of the e-Document in the e-File (optional)
  - Order of the e-Document in the e-File (optional)
- Folder:
  - Folder identifier
- e-File
  - Creation date of the electronic index
  - e-Document identification data

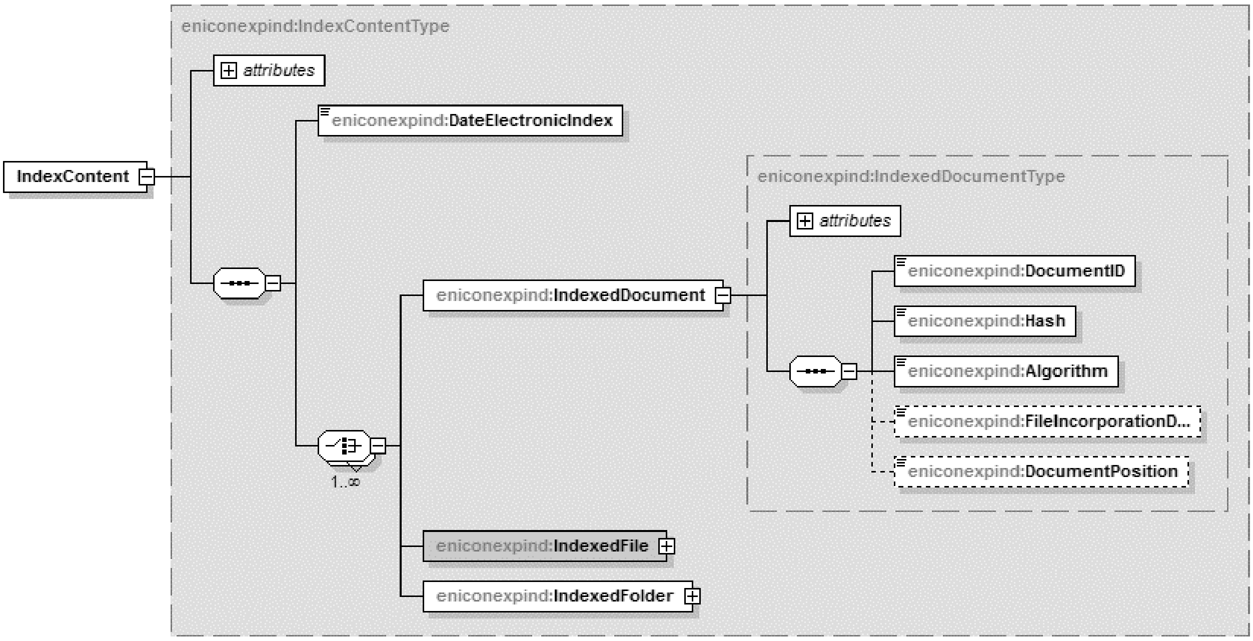
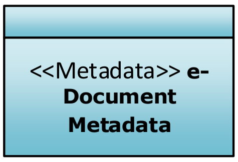

eniconexpind:IndexContentType
attributes
eniconexpind:DateElectronicIndex
IndexContent
eniconexpind:IndexedDocumentType
attributes
eniconexpind:DocumentID
eniconexpind:IndexedDocument
eniconexpind:Hash
eniconexpind:Algorithm
eniconexpind:FileIncorporationD...
1..∞
eniconexpind:DocumentPosition
eniconexpind:IndexedFile
eniconexpind:IndexedFolder

Figure 6: e-Index components

- The **e-Index signature** guarantees the authenticity and integrity of the content of e-Indexes (and therefore e-Documents) by public administrations, bodies or intervening agencies, in accordance with the regulations in force.

Metadata: e-Files metadata provides the minimum information required to identify the file such as its origin (source), legal validity and purpose, amongst others (the minimum Metadata required for the creation of e-Files can be found in The technical Interoperability Standards for e-Files). Further requirements regarding e-Files' metadata is addressed in the Semantic Layer, more specifically in the ABB- Business Process.

ABB- Metadata



SBB: e-Document Metadata

Requirements: Some of the main features regarding **metadata** the standard establishes are:

- It should comply with the Metadata Schema for the Management of the e-Document (e-EMGDE) that is to complement to the Technical Standard for Interoperability for e-Documents.
- It should be included in every e-Document exchanged in the public administration and public law entities (entities that carry out their activity according to the public law) associated or between such agencies or entities and citizens.
- It should not be altered at any stage of the administrative procedures except to correct errors.
- Complementary metadata can be added in response to special description needs and it should be agreed between the entities or bodies involved in the exchange of the information.
- The availability and integrity of metadata of documents and electronic files, maintaining permanent relations between each document and file and its metadata should be guaranteed.

The minimum required metadata for e-Documents can be found in the following table:

Metadata	Description/ Terms of use	Repeatability	Type	Value Schema
NIF version	Standard identifier of the version of the Technological Interoperability Standard for e-Documents (NTI), according to which the e-Document is structured	1	URI	http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e
Identifier	Standard identifier of the e-Document	1	Character Chain	ES_<organisation>_<YYYY>_<Specific ID>
Body	Standard identifier of the agency creating the document or capturing it	1:N	Character Chain	A single alphanumeric code for each body/unit/office extracted from the Common Directory managed by the Ministry of Territorial Policy and public administration.
Date of capture	Date when the document is entered in the document management system	1	Date/time	Format: YYYYMMDD T HH:MM:SS <ISO 8601>
Origin	Indication of whether the document has been created by a citizen or an agency	1	Logical	'0' Citizen '1' Administration
Production Status	Indication of the nature of the document, and of digitisation and format conversion in case of copies.	1	Character Chain	'Original' (Law 11/2007, Art. 30) 'Authentic e-copy with format conversion' (Law 11/2007, Art. 30.1) 'Authentic e-copy of paper document' (Law 11/2007, Art. 30.2 and Art. 30.3)

Metadata	Description/ Terms of use	Repeatability	Type	Value Schema
				‘Authentic partial e-copy’ Others
Format Name	Logical format of e-Document content type	1	Character chain	Value extracted from the list of accepted file formats in the Technical Interoperability Standard for Catalogue of Standards
Document Type	Description of the type of document	1	Character Chain	Decision Documents: Resolution, Agreement, Contract, Convention, Declaration. Transmission Documents: Communication, Notification, Publication, Acknowledgement of receipt. Proof of Documents: Deed, Certificate, Diligence. Judgement documents: Reports. Citizen’s Documents: Request Form, Report Form, Submission, Appeal, Citizen’s communication, Bill, Other. Others.
Signature Type	Indication of the type of signature attached to the document. In case of signature with a certificate, the signature’s format is indicated too.	1:N	Character Chain	‘CSV ’ e-Signature formats for e-Documents as defined in the Technical Interoperability Standard for Signature and Certification Policies in the public administration.
For Signature type = ‘CSV’				
CSV Value	Value of CSV	1:N	Character Chain	N/A

Metadata	Description/ Terms of use	Repeatability	Type	Value Schema
CSV Generation definition	Reference to the decree, resolution or document establishing the creation of the corresponding CSV.	1:N	Character Chain	For the General Administration (AGE) BOE (Official Spanish Gazette) reference: BOE-A-YYYY-XXXXX For others: corresponding reference
For Production Status: "Authentic copy with format conversion (Law 11/2007, Art. 30.1)" or "Authentic partial e-Copy"				
Original document identifier	Standard identifier of the original document the e-Document is a copy of.	1	Character Chain	If the original document is and e-Document: ES_<body>_<YYYY>_<specific ID>

SBB: e-File Metadata

Requirements: Some of the main features regarding **metadata** the standard establishes are:

- It should be associated during e-File creation for sending e-Files and making them available.
- It should not be altered at any stage of the administrative procedures except to correct errors.
- Complementary metadata can be added in response to special description needs. The complementary metadata should be applied in compliance with the provisions in the Technical Interoperability Standard for e-Document Management system.

The minimum required Metadata for e-Files can be found in the following table:

Metadata	Description/ Terms of use	Repeatability	Type	Value Schema
NIF version	Standard identifier of the version of the Technological Interoperability Standard for e-Documents (NTI), according to which the e-Document is structured	1	URI	http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e
Identifier	Standard identifier of the e-Document	1	Character Chain	ES_<organisation>_<YYYY>_<Specific ID>
Body	Standard identifier of the agency creating the document or capturing it	1:N	Character Chain	A single alphanumeric code for each body/unit/office extracted from the Common Directory managed by the Ministry of Territorial Policy and public administration.
File opening date	Date when the file is opened.	1	Date/time	Format: YYYYMMDD T HH:MM:SS <ISO 8601>
Classification	Administrative procedure the file is associated with.	1	Character string	Standard value schema according to the System of Administrative Information (SIA). If the procedure cannot be found in SIA : <Body>_PRO_<Specific_ID_PRO>3F[3]
Status	File status at the moment of the exchange.	1	Character String	'Open' 'Closed' 'Sending index closed'

Metadata	Description/ Terms of use	Repeatability	Type	Value Schema
Interested party	Identifier of the interested party	0:N	Character String	a) If a citizen or legal entity, ID/FIN/TIN or others. b) If public administration, <BODY UU>

I.1.1.5 Technical view

ABB- E-signing/Validation component

SBB: @Firma

Description: @firma is suite of solutions for identification and electronic signatures. It includes a multiple PKI Validation Authority offering validation services for qualified certificates and verification of electronic signatures to third relying parties, mainly eGOV applications. It provides support for transactions related to e-Document and forms signing/verification, citizens and business eID authentication, time stamping services and long term preservation signature formats.

Drivers: Facilitation of the implementation of the Spanish Law 59/2003 of the electronic signature, which allows multiple CSP (Certification Service Providers) to issue qualified certificates to citizens and business. @firma is a solution of reference for the identification and authentication described in chapter II of Law 11/2007, governing public electronic access to public services.

Specifications:

- @firma validates the electronic certificates issued by a qualified service provider of certification supervised by the Ministry of Industry, Trade and Tourism in Spain.
- Supported signature formats:
    - PKCS#7, CMS, CADES-BES, -T, -EPES, -C, -X, -XL, -A following ETSI TS 101 733 version 1.7.4 (2008-07); multiple signatures are supported.
    - XMLDsig, XADES-BES, -T, -EPES, -C, -X, -XL, -A, following ETSI TS 101 903 versions 1.1.1, 1.2.2 (only verification but not creation) and 1.3.2 (2006-03); for all formats enveloped, enveloping, detached and multiple signatures are supported.
    - PDF and ODF signatures, as well as ETSI PAdES profiles.

In order to foster interoperability and address multiple signature profiles enabled by optional fields in standard ETSI profiles (XAdES, CAdES, PaDES), the Spanish central government defines a specific signature policy [31] and uses -EPES signature profile to reference it for the validation purposes. The policy defines a set of criteria for public administration and its agencies in relation to electronic signatures, according to which the types of signatures allowed are the following:

- XAdES internally detached signature.
- XAdES enveloped signature.
- CAdES detached/explicit signature.
- CAdES attached/implicit signature
- PAdES

ABB- Trust Management Component

SBB: Secure Verification Code (CSV)

Description: The Secure Verification Code (CSV) is a term for the unique code that identifies an electronic document in the Spanish public administration. This alphanumeric code usually appears on all electronic documents issued electronically. The term was introduced by the Law on Electronic Access to Public Services (Law 11/2007). Specifically, the CSV is referenced in two articles of the Law:

- Article 18.1.b) : The Secure Verification code is linked to the public administration, body or entity and, where appropriate, to the person signing the document, in any case allowing verification of the integrity of the document by accessing the corresponding electronic office"

- Rule 30.5: "Copies made on paper of administrative public documents issued electronically and signed electronically will be considered authentic copies provided they include printing electronically generated code or other verification systems with which to compare its authenticity through access to files Electronic public administration, body or issuer."

Usage:

- **e-Files:** In the case of e-Files the e-Index signature has to be included in order to provide integrity and legal validity to the e-File and its content. This e-Index signature can be done:
    - Either by using an e-signature or electronic seal based on certificates, or

  - Using Secure Verification Codes. In this case the value of the CSV is included in the e-File as one of the minimum required metadata through the signature block. Furthermore, in order to improve the interoperability and exchange of documents and enable verification of the authenticity of e-Files without need to access the electronic office to collate the CSV, it is possible to consider the combination of the CSV with an electronic signature based on certificates.

- **e-Documents:** The main use of the CSV in the e-Document context is for the retrieval of the e-Documents from the electronic office by the citizen. The CSV will ensure that the printed e-Documents will be considered an official copy of the original one (when compared to the e-Document) and will provide legal validity to the copy.

SBB: @firma

Description: In addition to electronic signing/verification, @firma supports the validation of certificates issued (and thus signatures created by them) by trust certification service providers under the supervision of the Ministry of Industry, among them the national eID card. @firma component also validates e-Signatures generated by the e-Signing certificates from the national eID cards of the following countries: Austria, Belgium, Estonia and Portugal through mutual exchange of trust-lists. However, as far as e-Identification is concerned, @firma is able to interoperate with STORK in order to provide cross-country authentication services among the 15 member states that on-boarded on STORK project, as well as the pilots currently being carried out in STORK 2.0 project.

ABB- Identity Management Component

SBB: Citizen Authentication

Description: According to the Law 11/2007 (Articles 14, 15 and 16) the identification of a citizen/individuals in their relationship with the public administration can be done using the following:

- E-Signature systems/certificates included in the National Identity Card.
- Advanced e-Signature systems to identify and authenticate the documents.

- The government may determine, taking into account the data and affected interests, and always with justification, assumptions and conditions of use by citizens of other electronic authentication mechanisms. For instance, keys arranged in a previous record, information known by both parties, or other non-cryptographic systems.

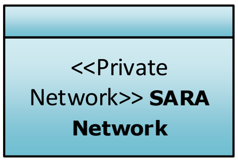
<<Identity Management component>> **Public Administration Authentication**

SBB: Public administration Authentication

Description: According to the Law 11/2007 (Articles 17, 18 and 19) the identification of public administrations in the exercise of their functions can be done using the following:

- Identification of Websites: The websites will use, in order to identify and ensure a secure communication therewith, authentication mechanisms based on certificates of secure device or equivalent.
- Identification and authentication of the public administration in automated administrative procedure:
  - **Electronic seal** of public administration, body or entity, based on electronic certificate that meets the requirements of the legislation on electronic signatures.
  - **Secure verification code (CSV)** linked to the public administration, body or entity and, where appropriate, to the person signing the document, in any case allowing verification of the integrity of the document by accessing the corresponding electronic office.
  - **E-Signature of the government employees in the public administrations:** The identification and authentication of the public administration, body or entity acting, when using electronic means, can be also done by electronic signature of their personnel. Therefore:
    - Each public administration may provide its personnel with electronic signature systems.
    - The electronic signature system based on the National Identity Card may be used for this purpose.

ABB- Private Network


<<Private Network>> **SARA Network**

SBB: SARA Network

Requirements: The communication network used for the document transfer should preferably be the public administration one. In this case, this network is SARA and its main aim is connecting networks of the Spanish government (central and regional) and European institutions facilitating the exchange of information and access to services.

I.1.2 GEISER- Integrated Registry Services Management

GEISER (Integrated Registry Services Management) is a comprehensive registry solution for any public organisation that provides services for the management of its input/output registration offices and for the reception of documentation and sending of the e-Documents to the Processing Units (the input/output registry offices are in charge of acknowledging the documents provided by the citizen (paper documents). They are scanned and a new e-Document is created in GEISER compliant with SICRES 3.0 specification).

The implementation of this solution is based on the SICRES 3.0[12] specification. As previously stated, this specification has been approved prior to the development of the National Interoperability Framework. This fact results in the existing of different schemas of data that need to evolve in order to provide an explicit and direct correspondence between both specifications. Therefore, the metadata used for e-Documents in GEISER may happen not to be related with the minimum data required by the National Interoperability Framework.

GEISER is a solution implemented by the Central Government that aims to provide a common platform for the reception and the output of the information/documents addressed to different departments of organisations and entities of the Central Government. Regional and local governments can also adopt this solution in their systems, but they can also develop their own.

The scope of GEISER is focused on the delivery of e-Documents to the processing units, then the processing and management of them is done through other platforms.

The main processes this solution comprises are "Creation" and "Access". Storing of e-Documents is currently carried out but it is not the main aim, and this functionality will tend to disappear when the solution is consolidated amongst users.

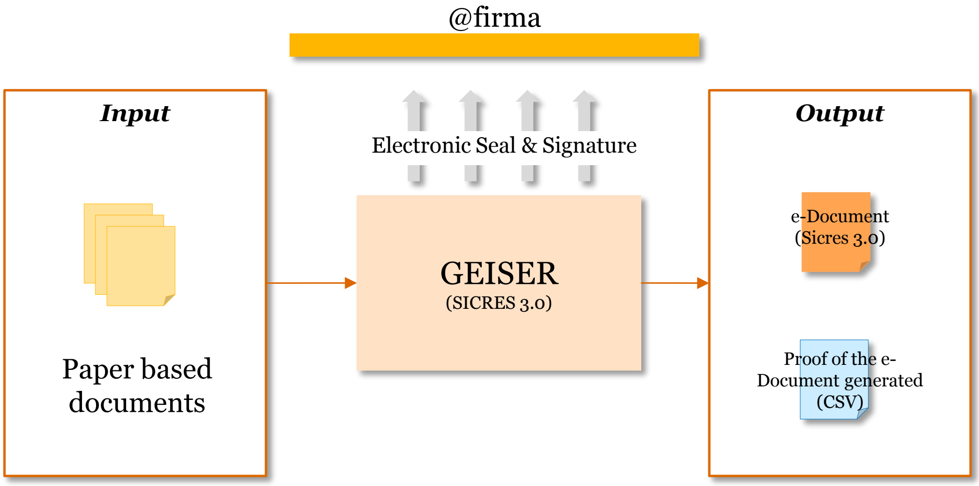


Figure 7: Geiser solution overview

[12] SICRES 3.0: It standardises and establishes a unique way, global and comprehensive data model for the exchange of information between registry entities regardless of the registry system origin or destination, and technology exchange.

I.1.2.1 Legal view

ABB Legal Requirements

SBB: Binding Legal Requirements

The implementation of GEISER responds to the **execution of the Law 11/2007**, more specifically, to the Article 24.4 of this law. According to this article, all the registry offices (referred in the article 38 of the Law 30/1992 on the Legal Regime of public administrations and Common Administrative Procedure) of the Central Government will be automated in order to ensure the interconnection of all these offices and enable the access by electronic means to the input/output registries and electronic copies of the submitted documents.

Regarding the legal validity of e-Documents generated from GEISER (as authentic copies) they have to comply with the requirements met in Specialisation: Legal Validity of e-Documents.

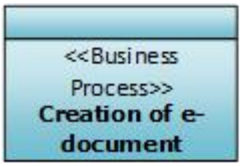
I.1.2.2 Organisational view

GEISER has been designed as a **horizontal solution** for all registration offices of the Central Government. It is widely implemented in different entities and organisations of the public administration and its configuration or security needs are not dependent on the kind of organisation that uses it.

GEISER does not cover the entire of the Administrative Process, its scope is limited to the input/output registry and the delivery to the processing units involved.

ABB- Business Process

As stated before, GEISER does not cover the entire Administrative Procedures, the main processes implemented in GEISER are the creation of e-Documents and the Access to them.



SBB: Creation of e-Documents

The creation of e-Documents is mainly performed in the input/output registry consists of two different phases regarding the actors involved:

1. **Citizen**

   The citizen fills the registry form and provides the documents to be digitised. All these documents have to include the handwritten signature of the citizen and corroborated with the ID of the citizen.

2. **Civil Servant - Input/output registry government employee**

   a. The government employee digitises the paper documents provided by the citizen (normally they are scanned).

   b. He approves and confirms that the electronic image derived from the digitisation complies with the requirements to be an "Official copy" of the original document.

   c. This information is integrated in GEISER.

3. **GEISER / Server**

   a. Each attached document is electronically signed (using CAdES - explicit) providing legal validity as an "authentic copy", with a seal from the SEAP (Secretary of State for public administrations).

   b. A proof of the entry is generated (normally is an e-Document in .pdf or can be generated on the fly).

   c. A CSV (Secure verification code) is generated for both, attached documents and the proof the entry.

   d. The proof is signed via PAdES with a seal from the SEAP.

4. **Civil Servant - Input/output registry government employee**

   The government employee provides the citizen with the proof of the entry registry and the CSV.

SBB: Access to e-Documents

Similarly to the creation, the access to the documentation is carried through different means regarding the actors involved:

1. **Citizen:** The citizen will have access to the documentation provided via Electronic Office Portal using the CSV provided with the entry proof and the registry number.

2. **Civil servants/Government employees:** The access to the documentation provided by the citizen is provided by GEISER (via Inbox) to the employees of

the processing units. The security of the access to the documents is managed by profiles with different access rights with the scope of the application.

SBB: Preservation of e-Documents

GEISER has been conceived as a solution to ensure the correct distribution of the documentation to the processing units and not as a document management system. However, documents are being stored in the platform. It uses Alfresco (document management system), although the next steps concerning storing of information will go through the elimination of Alfresco and evolving to the using of NAS (Network attached storage) for the storing of documents, with a main aim of not keeping documents in GEISER.

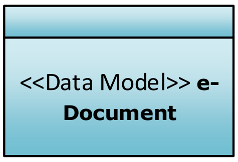
ABB- Actors

SBB: e-Documents' Actors

- Citizen as the main actor that triggers the processes implemented in GEISER.
- **Registry Offices:** They receive the documents and forms provided by the citizen and they create the e-Documents compliant with SICRES 3.0. As a later step, the documentation is inserted in GEISER for its delivery to the processing unit.
- **Processing Units:** Units in charge of processing the e-Documents from GEISER. They download the information and this is processed via other e-Document management solutions.

I.1.2.3 Semantic view

ABB- Data Model



SBB: e-Document

GEISER is implemented according to SICRES 3.0 which has been developed in a parallel way and it is focused to specific needs of the input/output registry. Therefore, the metadata contained in the e-Documents generated by GEISER does not need to match with the one in the National Interoperability Framework.

One of the specificities of GEISER (and of the information management by the input/output registry offices) is that only allows the citizen to provide documentation on a paper basis. In order to provide information on an electronic format other solutions are to be used (Common Electronic Registry[13]).

Considering these facts, the components of e-Documents managed by GEISER are the following:

- Electronic Image resulted from the digitisation of the document provided by the citizen.
- Electronic seal provided by the Administration.
- Metadata compliant with SICRES 3.0 specification.

The formats in which e-Documents are created in GEISER are the ones according to the Interoperability Agreement: Catalogue of Standards.

ABB- Metadata

SBB: Metadata

As stated previously, during the creation of an e-Document not all the descriptive metadata considered in the National Interoperability framework for SICRES 3.0 can be completed. The completion of the minimum required metadata will be carried out in two phases considering the actors involved in the registry and delivery processes. Therefore, some of the minimum required metadata will be completed in the registry offices, and the rest will be completed in the processing units.

Specifically the metadata involved in the creation of an e-Document in the registry office according to the SICRES 3.0 specification is the following:

- Description of the Annex (Name of the file).
- Document identifier

[13] Common Electronic Registry: It enables the submission of applications, texts and communications to the Spanish General Administration and its public bodies which fail to conform to administrative procedures already covered by the electronic registers of the various authorities. For example, a document compliant with a regional electronic register may not be compliant with the requirements for the Spanish General Administration Registry. Thus, the Common Electronic Registry adapts the document to these specific needs.

- Document validity
- Type of document
- Signature
- Timestamp
- Hash
- Mime type
- Additional Comments
- User that digitised the paper document

Table 2: SICRES 3.0 Metadata for the documents created in the registry offices

Metadata	Mandatory/Optional	Comments
Description of the Annex	Mandatory	Name of the original document/file.
Document/File identifier	Mandatory	-
Document Validity	Optional	It details the authenticity category of the document: - '01': Form - '02': Annex to the Form - '03': Original copy - '04': Original document
Type of document	Mandatory	It details the type of the document: - '01': Form - '02': Annex to the Form - '03': Internal document
Certificate	Optional	Certificate of the Annex (public key)
Signature	Optional	e-Signature of the Annex
Timestamp	Optional	-

Metadata	Mandatory/Optional	Comments
Validation OSCP of the certificate	Optional	Validation of the certificate used for signing
Hash	Mandatory	-
Mime type	Optional	Type of the Annex
Annex	Optional	Annex coded in Base64
Signed document identifier	Optional	If the Annex document is the signature of other document, it is necessary to specify the "document/file identifier".
Additional Comments	Optional	Additional comments of the Annex

I.1.2.4 Technical view

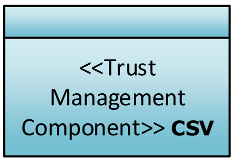
ABB- e-Signing / Validation component

SBB: @Firma

The sealing in the server is done using explicit CAdES that allows keeping the documents as independent files and the e-signature is kept as a different file (.csig), only the hash is signed. This process is carried out by a centralised service that uses the libraries of @firma.

Additionally, when the government employee provides the citizen with the proof of the submitted document, this proof includes the seal of the SEAP signed via PAdES.

ABB- Trust Management Component



SBB: CSV (Secure Verification Code)

In GEISER, the secure verification code (CSV)[14] is used, by the citizen, for consulting and retrieving the information via Electronic Office Portal. Thanks to the proof provided by the public administration to the citizen, the latter can track the evolution of its documents. Additionally, in case the citizen needs to print the e-Document derived from its relationship with the Administration, the CSV provides legal validity to the printed document.

[14] CSV creation specifications: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-3729

I.1.3 InSide

InSide is the solution implemented by the Ministry of Finance and Public Administrations to provide "Infrastructure and Electronic Documentation Systems". The implementation of this solution is based on the NIF specification.

InSide is a system for managing electronic documents and files so that they become compliant with the National Interoperability Framework and could be stored and / or be obtained according to these specifications. This management is based in generating the needed structures so that the e-Document or e-File is interoperable. However, the proper management of the documents is carried out by the administrative procedure's applications.

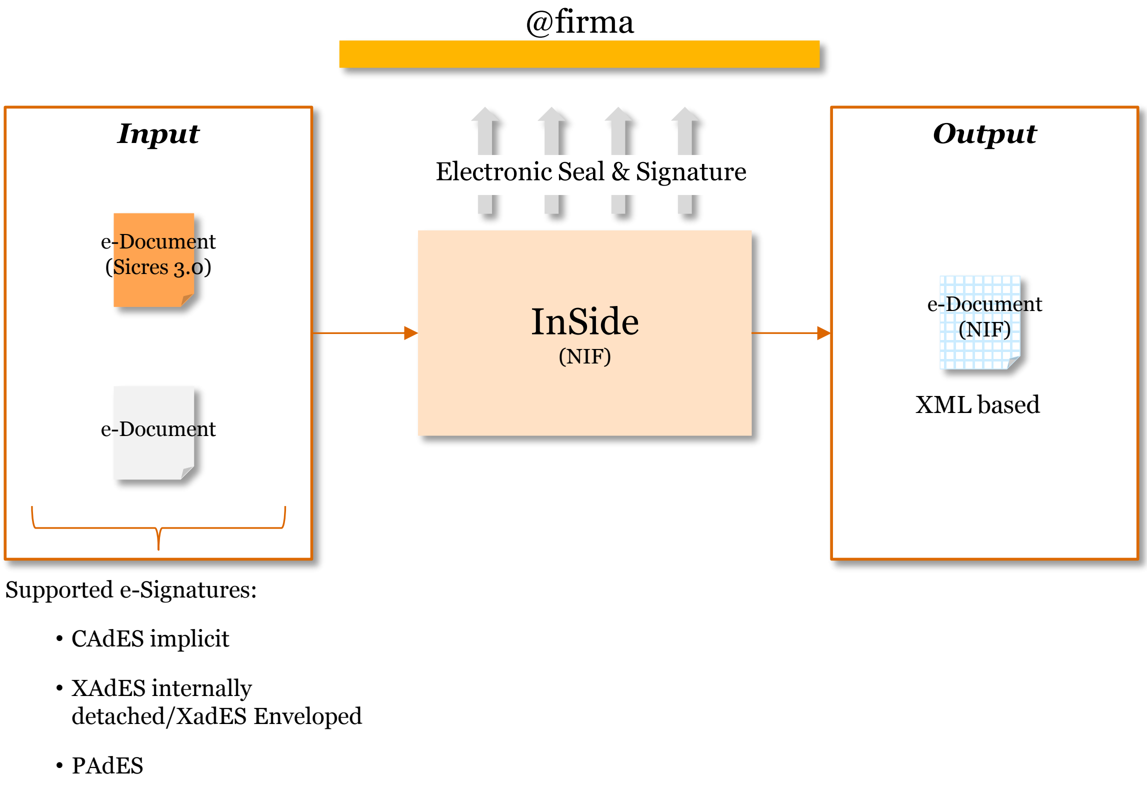


Figure 8: InSide solution overview

InSide consists of two different packages of functionalities that can be used either together or separately:

- **InSide Base**, which allows storing and modification of electronic documents and files in every document management system compliant with CMIS[15] [32], as well as the minimum required metadata established by the National Interoperability Framework. It also allows the validation and visualisation of documents and files for their using on a paper basis and the signatures of each managed document.

[15] Content Management Interoperability Services (CMIS) is an open standard that allows different content management systems to inter-operate over the Internet. Specifically, CMIS defines an abstraction layer for controlling diverse document management systems and repositories using web protocols.

- **G-InSide** (InSide Generator): It provides Web Services in the cloud SARA for the validation and generation of electronic documents compliant with the National Interoperability Framework, generation of PDF documents for the visualisation of electronic documents and files. For the generation, G-InSide takes as source an existing e-Document non-compliant with NIF and when a service from G-InSide is invoked it ensures that the structure, metadata and signature are compliant with NIF requirements. It includes the missing metadata or requires the e-Signature compliant with InSide requirements.

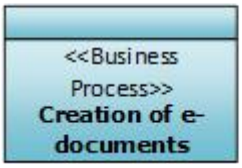
  It also provides with a set of services for the syntactic validation of the electronic documents and files.

I.1.3.1 Organisational view

Similarly to GEISER, InSide has also been designed as **a horizontal solution** within the Administrative Procedure. It is used in the public administrations as a horizontal solution in the basic Administrative process for generating e-Documents compliant with the National Interoperability Framework.

ABB- Business Processes

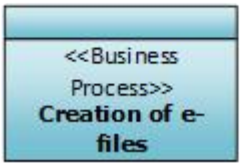
InSide does not cover the entire Administrative Procedure. The main processes implemented in InSide are the creation of e-Documents/e-Files, the validation/modification and visualisation.



SBB: Creation of e-Documents

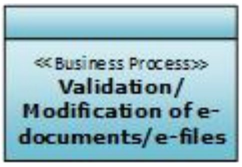
The creation of e-Documents in InSide takes as a starting point an existing e-Document generated in other stages of the Administrative procedure. The main purpose for managing this e-Document in InSide is the need to make it interoperable according to the NIF interoperability agreements. Therefore the steps followed are:

- Generate the XML structure according to which the new e-Document is going to be formatted. The original content has to be encoded in Base64 and in case the original document is signed, the signature should be CaDes, PaDes or XaDes. The structure of the InSide e-Document can be found in the **Anexo-Xsds de Inside-TipoDocumentInside.xsd** [33]**.**
- Generate the metadata. The minimum required metadata is included in the e-Document.
- The e-Signatures of the existing e-Document are analysed.



SBB: Creation of e-Files

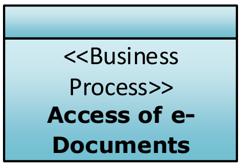
The creation of e-Files in InSide follows a similar process as the e-Documents (generation of XML structure, Metadata and e-Signature) with one exception. The process does not consider the content, it only generates the indexes of the documents without taking into account e-Documents contained by the e-File.



SBB: Validation/Modification of e-Documents/e-Files

The validation of e-Documents/e-Files ensures that the structure generated (XML file containing the original content, the metadata and the e-signature) is compliant with the NIF. For that purpose, the final structure is validated against the XSD of the NIF.

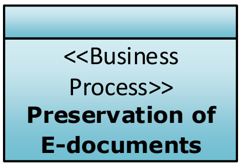
The structure created for e-Documents and e-Files can be modified and corrected under InSide as long as the status of the e-Document is not "closed". Additionally, InSide allows versioning and tracking of the e-Documents and e-Files that are stored within the application.



SBB: Access (visualisation) of e-Documents

This functionality allows the access and visualisation of a NIF document. The result is a .pdf document where the following information is specified:

- **Metadata:** NIF version, Identifier, Bodies, Capture Date, Origin, Production Status, Type of Document and the additional metadata (if any).
- **Information about the e-Signatures:** Type, signee, CSV, e-Signature Date and CSV regulation.
- **Content of the e-Document.**



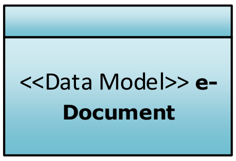
SBB: Preservation of e-Documents

InSide does not consider e-Archiving as part of the e-Document/e-File management process and it does not integrate with an e-Archiving service provided by other solutions. However, it considers the storing of documents while they are being processed through InSide Base.

I.1.3.2 Semantic view

ABB- Data Model

InSide can manage two types of electronic "entities":

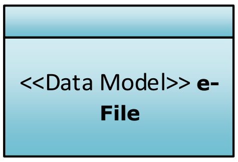


SBB: e-Document

e-Documents as independent documents, that consist of:

- **Content.** The content of e-Documents should be included in base64 according to one of the available encoding standards specified in the **Technical Interoperability Standard for the Catalogue of Standards** [30].
- **e-Signature.** The signatures allowed in the incoming e-Documents are CAdES, PAdES or XAdES and they must include the content of the e-Document. The structure created by InSide is XML based, therefore the signature to be used to sign InSide e-Documents is XAdES.
- **Metadata**

The incoming document InSide uses as a source can be electronically signed or not. If it is signed, the document should be contained in the signature file and the types allowed are CAdES, PAdES or XAdES. In the new InSide e-Document, compliant with NIF, the content (electronically signed or not) should be included in Base64. The InSide e-Document has a XML based structure and therefore is signed using XAdES.



SBB: e-File

e-Files that according to the Technical Interoperability Standard they are composed of

- **e-Documents** that should comply with the structure and format specifications in the Technical Interoperability Standard for E-documents. E-documents can be part of e-Files as independent elements or in folders, being sets of e-Documents created for functional purposes, or as part of another file, embedded in the former.

- **e-Indexes** that will guarantee the integrity of e-Files and their retrieval when necessary. E-indexes should contain the whole set of e-Documents associated with a file at a given moment and, if necessary, their distribution in folders or files.

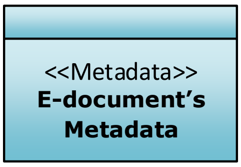
  The index contains a hierarchical representation of the file. It can contain the date of the index, which if it comes empty is automatically generated by G-InSide with the value of the current date.

  It may also contain other indexed items:

  1. The index of another file
  2. An indexed document. In this case, it should indicate:
     a. Document identifier (required).
     b. Function summary with which the footprint of the document has been calculated (required).
     c. Hash document (required).
     d. Order of the document in the file (optional).
     e. Date of incorporation to the file (optional)
  3. An indexed folder, in which case the identifier of the folder should be indicated. InSide it can contain indexed items (another index, another indexed folder or indexed documents).

- **e-Index** signature by public administration, body or agency in accordance with the regulation in force.
- **Metadata**

ABB-Metadata



SBB: e-Document's Metadata

a) **Creation** of an e-Document in InSide:

The metadata required to create/register a new e-Document is a subset of the minimum required metadata established in the Technical Interoperability Standard for e-Documents. However, the metadata needed is different if the e-Document is being created directly in InSide or if it has to be converted to NIF format.

The metadata needed in both cases is detailed in the following table:

Type of metadata	InSide e-Document	Conversion to NIF format
Minimum required Metadata	• Body • Date of capture • Source: Citizen/Administration • Document type	• Identifier • Body • Source: Citizen/Administration • Document type • Production Status
	The rest of the required minimum metadata will be deduced by InSide, such as Format Name or NTI Version.	The rest of the required minimum metadata will be deduced by InSide, such as Format Name or NTI Version.
Additional Metadata	Additional metadata can be included according to the National Interoperability Standard.	

The creation of new e-Documents in InSide can be done according to different sub-processes, here, the metadata associated to each process is detailed:

Process	Source	Metadata	Metadata Value	InSide Value (for NTI docs)
New Registry	Original	Production Status	"Original"	EE01
Authentic e-Copies in a different format	Existing e-Document	Production Status	*"Authentic e-copy in a different format"*	EE02
Authentic e-Copies of paper documents[16]	Paper document	Production Status	*"Authentic e-copy of a paper document"*	EE03
		Identifier of the source e-Document		
Authentic e-Copies of parts of documents	Existing e-Document	Production Status	*"Authentic e-copy of a part of a document"*	EE04
		Identifier of the source e-Document		

[16] An authentic e-Copy of paper documents responds to the process of creating an e-Document from the digitisation of a paper document and then obtain a printed authentic document from the e-Document the Administration has. However, a New registry may imply that the original source can be electronic (e.g. online application forms) that are directly handled by electronic means.

b) The **modification** of e-Documents implies that either metadata or/and content can be modified. This means that a new version of the e-Document will be created. For this purpose, the only mandatory parameter needed is the document itself, which contains the identifier, the NTI metadata and additional metadata (when completed).

c) The **access** (visualisation) of e-Documents will retrieve the following data:

- Content
- Minimum required metadata
- Additional metadata included
- e-Signatures

In order to get this information, input parameters are needed:

- e-Document identifier
- e-Document version (optional)

<<Metadata>>
E-file's Metadata

SBB: e-File's Metadata

a) **Creation** of an e-File:

Similarly to e-Documents, the metadata required to register a new e-File is a subset of the minimum required metadata established in the Technical Interoperability Standard. As well as in e-Documents, the metadata needed for the creation of e-Files is different if the e-File is being created directly in InSide or if it has to be converted to NTI format.

The metadata needed in both cases is detailed in the following table:

Type of metadata	InSide e-File	Conversion to NTI format
Minimum required Metadata	• Body • Classification	• Identifier • Classification • Status • Body • Creation Date

Type of metadata	InSide e-File	Conversion to NTI format
	• If "Elaboration Date" is not included, it is filled with the time of the registry. • Status = "Open"	The rest of the required minimum metadata will be deduced by InSide, such as Format Name or NTI Version.
Additional Metadata	Additional metadata can be included according to the National Interoperability Standard.	

b) The **modification** of e-Files may imply different tasks to be carried out that may result in different workflows, as detailed in the following table:

Type of modification	Input	Output	Additional task to carry out as a consequence of the modification
e-File modification	• e-File Index • Minumum required metadata • Additional metadata	• e-File identifier • New version number	None
e-File Metadata modification	• e-File identifier • Minumum required metadata • Additional metadata	• e-File identifier • e-File status • New version number	None
e-File Status	• e-File identifier • Minumum required metadata	• e-File identifier • e-File status • New version number	In case the e-File Status = "Closed", the e-File index will be signed and a copy of the generated index will be stored.

c) The **access** (visualisation) of e-Files will retrieve the following data:

- Signed e-Index of the file
- Minimum required metadata
- Additional metadata included
- Visualisation of the e-File index

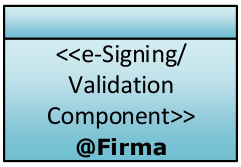
In order to get this information, input parameters are needed:

- e-File identifier

- e-File version (optional)

I.1.3.3 Technical view

ABB - e-Signing/Validation Component



SBB: @Firma

The e-Signing process is carried out using the services provided by SBB: @Firma.

SBB: @Firma

In the case of InSide, the types of e-Signatures allowed from the incoming e-Document are:

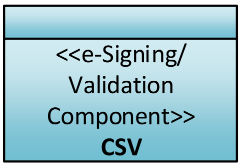
- PadES: PDF Advanced Electronic Signature.
- XadES internally detached/XadES Enveloped: XML Advanced Electronic Signature.
- CadES: CMS Advanced Electronic Signature which is a set of extensions to Cryptographic Message Syntax (CMS).

These signatures will embed in content of the e-Document.

Since the structure created by InSide is XML based, the e-Signature to be applied is XAdES.

Additionally it is also possible for InSide, to create **a server side electronic sealing** of the content by using @firma services.

ABB- Trust Management Component



SBB: CSV (Secure Verification Code)

The access and retrieval of the information can be done using a **Secure Verification Code (CSV).**

I.1.4 @Doc - Services Platform of Electronic File

@Doc provides a horizontal services platform for e-File and e-Document management that enables client applications to incorporate easily much of the requirements of the NIF interoperability agreements on Technical Standards for e-Documents. The main purpose is to facilitate the interoperability and is not meant to manage business processes.

The platform ensures the store, recovery and long-term conservation of the electronic files.

@Doc is conceived as a bus of services where data structures are exchanged using web services. These data structures must be consistent with the xsd schemas published in the Technical standards for Electronic File and Electronic Document.

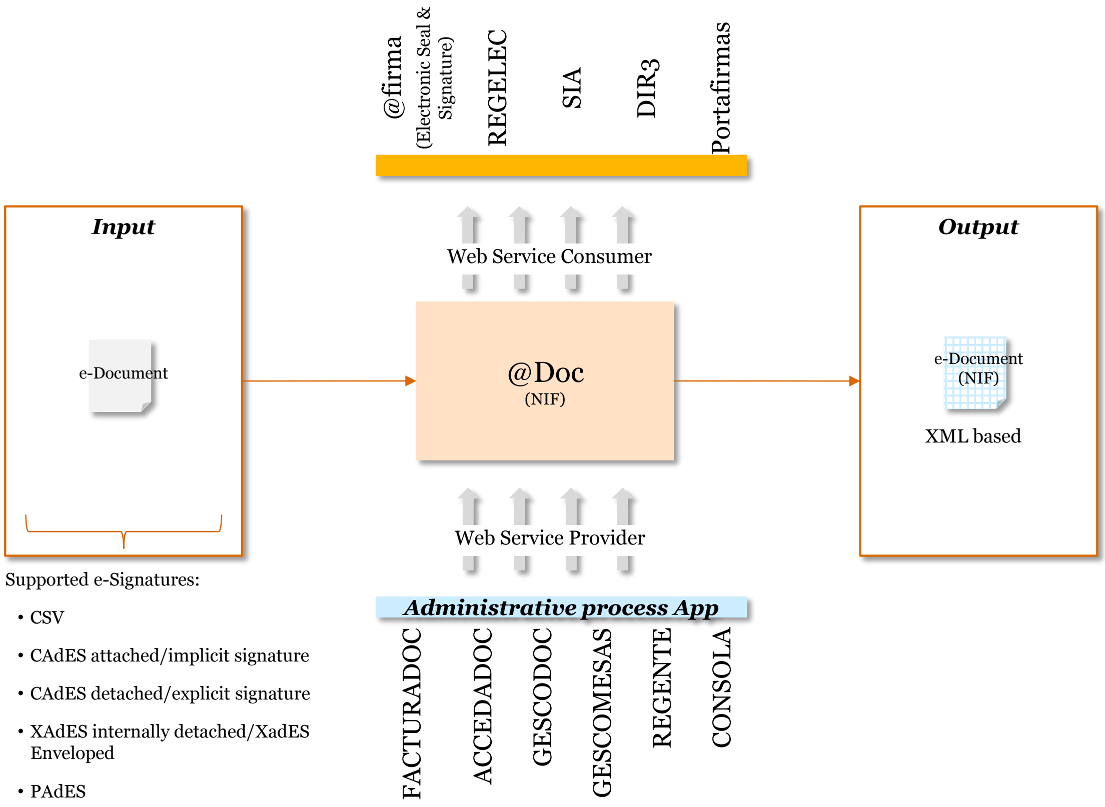


Figure 9: @Doc solution overview[17]

[17] Solutions @Doc integrates with:
REGELEC: Horizontal platform for the management of electronic registry records under SICRES 3.0.
DIR3 (Common Directory): The common directory provides a consolidated inventory, common to the whole administration of functional units / public bodies, their offices and units associate economic management, budget - facilitating the maintenance and co-leader of information.
SIA: It is the inventory of administrative information from State Central Government, regulated by article 9 of the National Scheme for interoperability, and updated in a co-leader by all agencies participants. It contains the connection of procedures and services of the Spanish General Administration and the different Public Administration participants.

The following figure shows the high level architecture for @Doc described in the Platform description document (in Spanish).

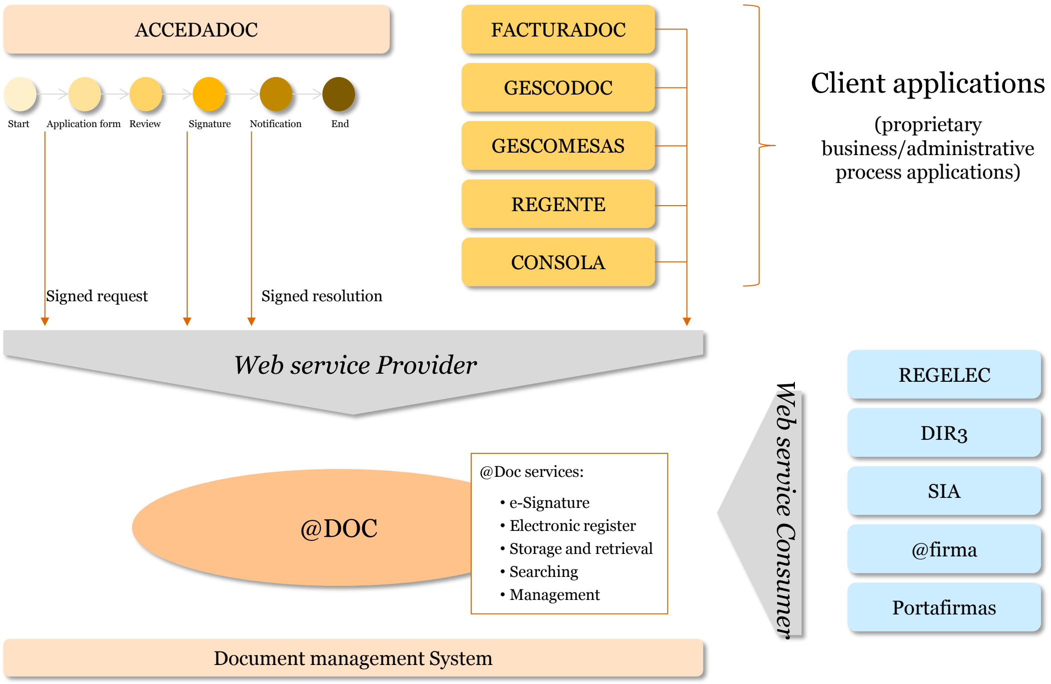


Figure 10: @Doc high level architecture

@Doc is designed to operate in a multi-agency environment. This means that @Doc can be configured to respond to the specific needs of each organisation. Therefore, it is possible to set the parameters accordingly to the needs of each Administration/entity/body. Some of these configurable parameters are the following:

- Independent keystores (containing the private key) for the e-signatures certificates of each public entity.
- Configuration of the electronic seal format and algorithm applied to the file e-Index and the documents contained in it (separately).
- Possibility of generating EPES profiles for electronic seals including the information of a particular signature policy.

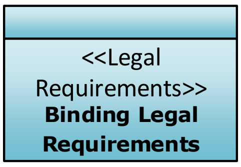
Portafirmas: Information system developed by the Ministry of Industry, Energy and Tourism for electronic signatures of documents (XAdES format).
Notific@: Notific@ is a hub of communications and notifications in a common format. @Doc has just finished its integration with Notific@ in testing environment.
ACCEDADOC: ACCEDA is a platform composed of three main functionalities: managing the content of electronic site, managing the interface with the citizen to initiate and consult states of cases involved in the same as well as a complete processing backend electronic records. The version that provides the integration with @Doc is ACCEDADOC.

- Enable/disable of automatic validation of electronic signatures associated with documents.
- Parameterisation of text, logo and dimensions of the bar code which represents the CSV in the authentic copies.
- Enable/disable validation of stakeholders' codes.
- Enable/disable of format content coherence of the document with 'Format Name' metadata.

The complete list of configurable parameters can be found in the integration manual of @Doc (in Spanish).

I.1.4.1 Legal View

ABB- Legal Requirements


<<Legal Requirements>>
Binding Legal Requirements

SBB: Binding Legal Requirements

The implementation of @Doc facilitates the policy compliance associated with **the Law 11/2007: Royal Decree 1671/2009** and the Interoperability Agreements from the National Interoperability Framework.

The RD 1671/2009 enacts Law 11/2007, of electronic access of citizens to public services in the field of the Spanish General Administration and public bodies linked or dependent on it. It entails data transmission, electronic and general point of access, identification and authentication, electronic records, communications and notices and electronic documents and copies.

Aspects covered by @Doc with regard to these policies are:

- Electronic File [34]
- Electronic Document [26]
- Authentic Copy and Electronic Document Conversion [35]
- Document Digitisation [36]
- Electronic Signature and Administration Certificate Policy [37]
- Data Model for exchanging entries between Registry Entities [14]
- Catalogue of Standards [30]

I.1.4.2 Organisational View

@Doc has been designed as a **horizontal platform (bus of services)** for the implementation of electronic files services in different organisations and it allows the integration with different applications that implement various business/administrative processes of the organisation. It does not include the business logic for the content management and document/file processing.

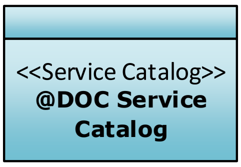
@Doc offers a solid infrastructure to store and recover electronic files. It provides a service catalogue that allows vertical applications to implement the requirements of the electronic file policy.

The platform ensures security mechanisms during the data and documents transfer and provides homogeneous methodologies to process the electronic signatures of the repository documents.

It enables setting up certificates and own user entity logo, signature format parameters, validations, entity codes, etc.

@Doc facilitates the integration with other horizontal platforms developed either by the same body or different ones: Electronic Registry, @firma, SIA, DIR, Portafirmas, etc.

ABB- Service Catalog



SBB: @DOC Service Catalog

The current version of the platform provides five service descriptors with multiple methods:

- **Administration Services:** Management Methods for client applications and platform status. They allow the implementation and maintenance of new client applications without additional coding and without stopping the platform. The implementation service receives the complementary metadata definition of the new client application and deployed the document types for the Document Management. Web services are provided for the consultation of the deployment status, the platform status and the administrator password management.
    - Registration and update of client applications: access credentials, responsible person data, configuration parameters to store for electronic seal, electronic seal format and signature of the index file, dynamic deployment of extended types of document and file with complementary metadata, configuration parameters of authentic copies, configuration parameters of validations.
    - Data Query of client application
    - Modification of administration access credentials (encrypted key)
    - Querying of client applications deployment
    - Consultation of the platform status (version deployed, date of deployment and time since last server boot)

- **Electronic File and Electronic Document Services:** Methods for inserting, updating and searching for electronic files and electronic documents, electronic signatures and authentic copies.

    - Insertion services: creation of electronic file and electronic documents in any state of preparation (original files, electronic copies with changes in format, partial copies, etc.). @Doc verifies the minimum mandatory metadata for the files and documents, checking the SIA and DIR specifications. It manages automatically the update of the file Contents and its electronic sealing.
    - Update services: updating the minimum mandatory and complementary metadata for electronic files and electronic documents. Updating the content of documents and control of versions.
    - Deletion services: elimination of documents and file when the production status of the file is the appropriated (different from closed).
    - Consultation services: recovery of metadata of files and documents. Obtaining content and electronic signatures associated to a document. Recovery of versions of content of a document.
    - Copies Generation services: generation of paper Authentic Copy with inclusion of CSV (Secure Verification Code), partial copies and copies with changes in the format.
    - File Life-cycle services: closure and numbered of the file, referrals management.
    - Search services: search for electronic documents and files using either indexed content or combinations of criteria for minimum mandatory and complementary metadata.
    - Electronic signature services: Validation of signatures associated with the electronic documents, verification of electronic seals, verification of CSV, generation of CSV and electronic seals.

- **Electronic Invoicing (Facturae) Services:** Methods for the verification of accounting data, structure and signing of documents in Facturae formats [38] (in Spanish) (3.0, 3.1, 3.2 and 3.2.1) and generation of paper authentic copies of invoices. Additionally, extensions have been incorporated to the services of insertion, update, obtaining and search of electronic documents to include Facturae features. Among which all the metadata referred in the accounting registry of Invoices web services are included.

- **Directory Services:** Consulting data obtained from the DIR3[18].

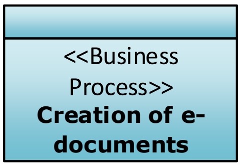
- **Registration Services:** (optional) services for the generation and recovery of recorded entries complying with SICRES 3.0 specification. @Doc is integrated with the Electronic Register of the Ministry of the Presidency.

[18] DIR3 (Common Directory): The common directory provides a consolidated inventory, common to the whole administrationm of functional units / public bodies, their offices and units associate economic management, budget - facilitating the maintenance and co-leader of information. http://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=dir3#.VNilq-90wiQ

- **Portafirmas Services:** (optional) services for requesting the submission of a document inserted into an electronic file to the Ministry of the Presidency Portafirmas.@Doc manages the recovery of the electronic signature from the Portafirmas application, its verification and automatic inclusion in the electronic file and the notice of available signature to the client applications through callback.

ABB- Business Process

Main processes for Electronic File and Electronic Document Services are descripted below:



SBB: Creation of e-Documents and e-Files

Insertion process is available for e-flies and e-Documents. It is carried out in collaboration with the client application platform (e.g. ACCEDADOC), which creates the e-Files and specifies some of the minimum required metadata and the complementary metadata. The minimum required metadata is specified by the client application (e.g. Organisation, Type) and by @Doc that automatically provides metadata such as the identifier or the opening date. Then, @Doc platform includes the specific metadata and validates the e-signature. After that, it generates a paper authentic copy that is returned to the client application and it is delivered to the citizens.

The following picture presents the sequence for the creation process using as an example the submission of an application form through the electronic government site:

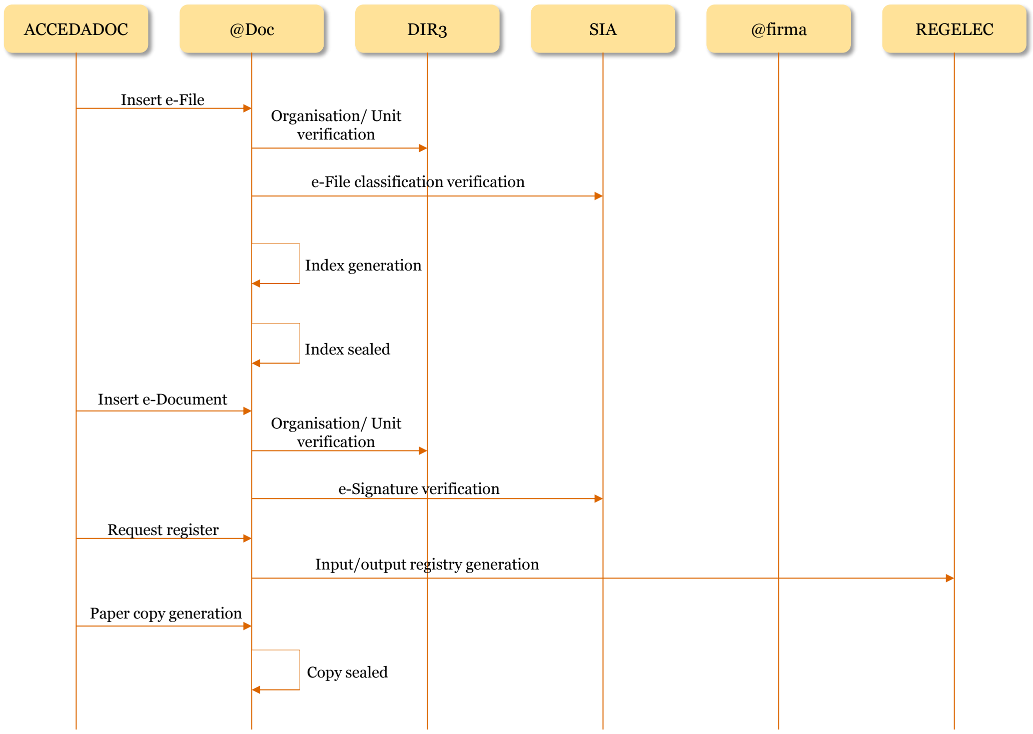


Figure 11: e-File creation process originated by the submission of an electronic application form

<<Business Process>>
Modification of e-documents

SBB: Modification of e-Documents and e-Files

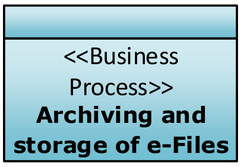
Updated and deletion process allows to change or delete metadata, contents and signature for e-Documents when the status of the file is the appropriated (status of the e-File or e-Document different from closed). If the document belongs to an e-File, after the update and deletion processes are executed, the index is updated and the document is resealed to maintain the integrity.

<<Business Process>>
Access to e-documents

SBB: Access to e-Documents and e-Files

Consultation process using e-Document or e-File identifier requires the client application to have set the e-Document identifier.

Searching process can be based on metadata or indexed content for e-Documents. In the case of a PDF file, it is necessary the existence of text layer. This is a configurable option of the digitalisation process that allows adding a structured content layer over the original non-structured content (e.g. a text layer over a scanned document). However, @Doc does not provide the functionality for managing OCR processes. This is mainly done by the external applications and @Doc can perform the indexation and perform the searching.



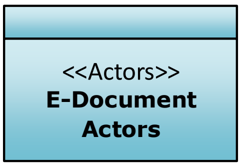
SBB: Archiving and storage of e-Files

The storage process is delegated on the document management system (external system). @Doc provides interconnection with the DMS for long-term storage of e-Files.

The archiving process is managed in the transitions between the different states of the e-Files during archiving.

The archiving represents the last stage of the e-Document/e-File lifecycle. It includes processes such as conversion to PDF/A, reporting of conversion to PDF/A or generation of documentation for third parties consultation (with the generation report...). However, the e-Archiving process is not implemented in the current version of @Doc. It is planned for the 2.0 release (currently in beta testing).

ABB- Actors



SBB: e-Document Actors

The platform is currently being used by the Ministry of the Presidency and its autonomous bodies, CIS and CEPCO.

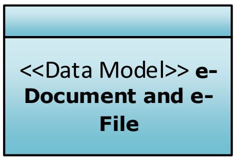
Additionally, the following bodies have showed their interest in @Doc:

- Ministry of Industry
- Ministry of Education
- Junta de Castilla La Mancha
- Junta de Castilla y León
- Xunta de Galicia
- Basque Country University
- Zaragoza University

- Private and semi-public companies: Tecnocom and Indra.

I.1.4.3 Semantic View

ABB- Data Model



SBB: e-Document and e-File

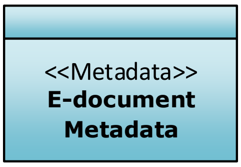
The business entities used in @Doc are e-Files (SBB: e-File and e-Documents (SBB: e-Document) with the structure defined in the I.1.1 Interoperability agreements for e-Documents.

The formats in which e-Documents are handled in @Doc are the ones according to the Interoperability Agreement: Catalogue of Standards.

The formats in which e-Files are handled in @Doc are the ones according to the Technical Interoperability Standard for e-Files.

@Doc allows the generation of referral and reopening sub-file.

ABB- Metadata



SBB: Metadata

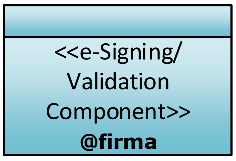
Metadata involved in the platform processes are:

- Minimum required metadata according to the Interoperability Agreements for electronic file and electronic document (Complementary metadata according to specific needs).
- @Doc specific metadata: (LatestModificationDate)
- Digitalisation metadata
- Specific metadata of every client application integrated with @Doc
- Invoice metadata (electronic invoice and documents with Facturae format)

It is relevant to outline that for the second release of @Doc, @Doc 2.0, the exchange and archiving business processed will be implemented and the metadata used for this purpose is according to e-EMGDE (Metadata Schema for the management of the e-Document).

I.1.4.4 Technical Layer

ABB- e-Signing / Validation component



SBB: @firma

The e-Signing process is carried out using the services provided by miniapplet libraries from @Firma are being used to reuse code between public administrations. E-Signature validation is delegated to @Firma.

In the case of @Doc, the types of e-Signatures allowed are:

- CSV
- PadES.
- XadES internally detached / enveloped.
- CadES attached/implicit / CAdES detached/explicit.

Sealing is configurable for each client application regarding:

- The certificate store to apply the seal.
    - The existence of independent keystores (containing the private key) allows the application of the appropriate electronic seal to the e-Document or e-File according to the processing unit. It stores the relationship between the bodies/entities integrated in @Doc and the type of certificate they use. Once the type of certificate to seal the document has been chosen, the validation is done using @firma libraries. Additionally, the encryption of the access passwords for the keystores is based on asymmetric cryptography.
- The electronic seal format.
    - It is possible to use any of the formats specified in the Signature and Certificates Policy of the Interoperability Agreements. The document contents format has to be consistent with the signature format selected (for example, to apply a PAdES seal is necessary to have a PDF document).
      It can also be set a main signature format and an alternative one. This enables to use a PAdES seal format if the document is PDF and another signature format (XAdES or CAdES) for other format document.
- Hash generation algorithm.

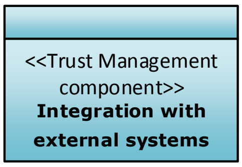
All the information above applies to the e-File index sealing.

ABB- Trust Management Component

SBB: CSV (Secure verification code)

The generation and verification of the secure verification code (CSV)[19] are offered as part of the Electronic Signature services. The CSV is also included in the generation of paper Authentic Copy.

ABB- Orchestration Service


<<Trust Management component>>
Integration with external systems

SBB: Integration with external systems

The integration of @Doc with external systems is implemented through web services. @Doc provides web Services so that other solutions can use the services offered by @Doc. At the same time, @Doc uses web services provided by other solutions (e.g. @firma) to be able to offer some of its functionalities [39] (in Spanish).

The external systems integrated with @Doc are presented below:

- **Directorio Único de unidades orgánicas y oficinas (DIR) – Unified directory of organic units and offices -**
  - DIR Synchronization processes allows updating offices and entities DBs exploited by the platform.
  - Verification of organisational unit codes related to the electronic files and documents
- **Sistema de Información Administrativa (SIA) – Administrative Information System -**
  - SIA dynamic consultation via web services to verify the classification codes associated to the electronic files

[19] CSV creation specifications: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-3729

- **@firma**
  - Dynamic validation of the electronic signatures of the electronic documents provided by the client applications (configurable).
  - Obtaining certificates information.
  - Control of seal and e-signature formats admitted by Electronic Signature and Administration Certificate Policy [37].
  - Use of libraries from @firma (v 3.3) for electronic sealing.
- **Registro Electrónico (REGELEC) – Electronic Register**
  - Applications using @Doc have electronic registration services adapted to SICRES 3 without the integration with REGELEC
  - Generation and recovery of input/output entries based on e-File.
  - Use of Electronic Registration services is optional
- **Portafirmas (Ministry of Presidency)**

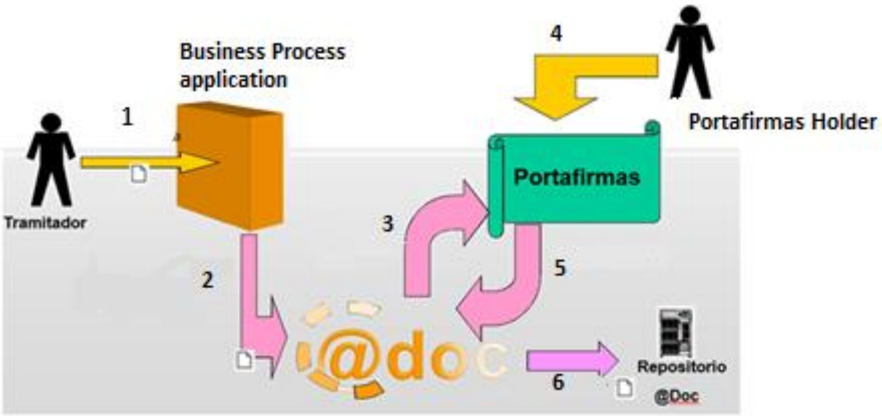


Figure 12: Integration of @Doc with Portafirmas system

1) The government employee acknowledges that the e-Document in process needs the e-Signature of the owner of the e-Document.
2) The e-Document is stored and the request for the e-Signature is sent.
3) @Doc submits the documents to be signed to the specific Portafirmas holders (owners of the e-signatures requested by the system).
4) The Portafirmas holder signs electronically the e-Document.
5) @Doc recovers the e-Signature included in the electronic file.
6) @Doc provides a callback notification to the client application. This notification provides information about how the e-Signing process has been carried out (e-Signature accepted or rejected).

7) @Doc generates e-Signature proof. The proof follows paper authentic copies format and includes a CSV.

I.1.5 XML Schemas in Spain

This section details the XML Schemas used in Spain for the exchange of e-Documents and e-Files according to NIF standard. These schemas are widely explained in the User Manual for the exchange of e-Documents and e-Files (in Spanish), which explains the structure and components the e-Documents and e-Files should have. It provides different structures/schemas according to the different standards upon which e-Documents can be built.

Among the Schemas described in this document, the following can be found:

- XML Schema for e-Document content: Articles 67, 68, 70 and 72.
- XML Schema for e-Document metadata: Article 73.
- XML Schema for e-Document signatures:
  - CSV signature: Article 78.
  - XAdES internally detached: Article 79.
  - XAdES enveloped: Article 80.
  - CAdES detached: Article 82.
  - CAdES attached: Article 83.
  - PAdES: Article 84.
- XML Schema for e-File exchange: Articles 105 and 110.

I.2 Estonia

I.2.1 Estonia Document Management System

I.2.1.1 Introduction

The Estonian government relies on a multi-layer architecture in order to realize e-Document processes. These layers satisfy diverse functional aspects of e-Document processes; namely e-Document generation, consumption, signing, routing, signature-verification, encryption, decryption, metadata enrichment, searching, short-term preservation and long-term preservation. It could be argued that these layers are hierarchical; which implies functional inheritance i.e. specific functionality of the underlying layers is inherited to the upper ones. However this functional inheritance is not in the scope of our research. These layers include:

- a) the X-Road layer
- b) the Document Exchange Center (DEC)
- c) the DigiDoc layer and
- d) the Estonian e-Identification layer

In the frame of our analysis, the e-Document is defined as a payload-agnostic entity which may consist of structured or unstructured data used in the context of an administrative process. This definition is totally applicable in the Estonian case since the existing deployed tools that comprise the various layers can support the lifecycle of both structured and unstructured data.

The complementarily of the four layers is depicted in the figure below (see Figure 13). In a nutshell, the X-Road system is used in order to facilitate the transport layer of e-Documents between several endpoints (publishers and subscribers). It also provides the adaptation mechanisms that are required for database interconnection. On the other hand, the e-ID framework is used in order to allow an end-user to identify him/herself all across the lifecycle of document management process (creation, routing etc). Some essential horizontal functionality that is related to e-Documents are electronic signing, verification, encryption and decryption. All these are tackled by the DigiDoc layer. Finally, metadata-based routing is achieved using the DEC layer.

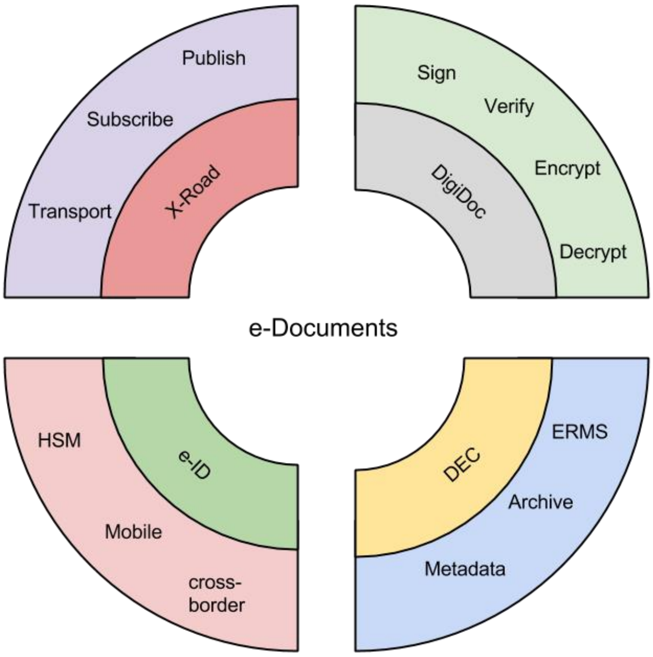


Figure 13: Tools Complementarity

A more elaborated view on these layers is provided in the following chapter where the technical layers are discussed.

I.2.1.2 *Short overview of the technical layers*

X-ROAD layer

X-ROAD is the invisible yet crucial environment that allows the nation's various e-services databases, both in the public and private sector, to link up and operate in harmony. One of the key elements of e-Estonia is that its databases are decentralized, which means:

- There's no single owner or controller.
- Every government agency or business can choose the product/service that's right for them.
- Services can be added one at a time, as they're ready.

X-ROAD architecture is provided on Figure 14.

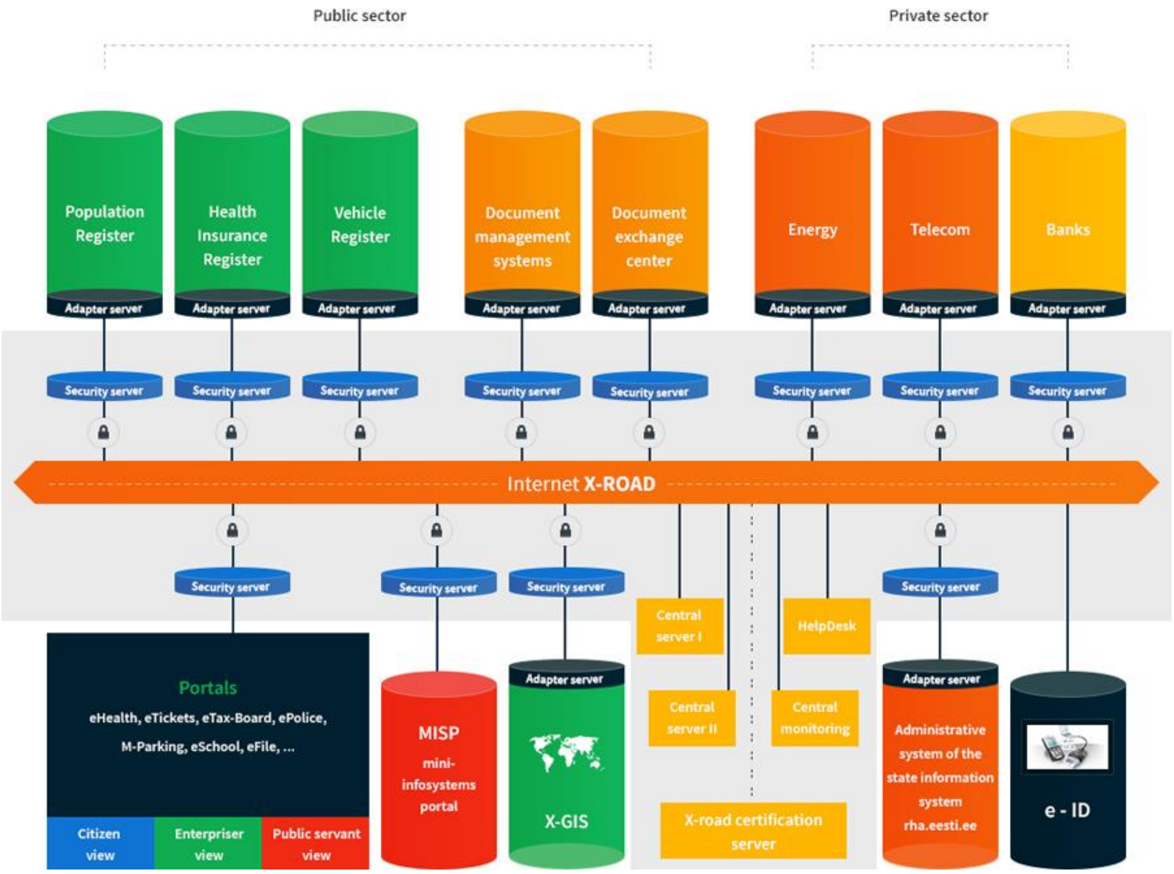


Figure 14: X-Road Architecture that highlights the inter-linking capabilities

X-Road is the all-important connection between these databases, the tool that allows them to work together for maximum impact. All of the Estonian e-solutions that use multiple databases use X-Road. Originally X-Road was a system used for making queries to the different databases. Now it has developed into a tool that can also write in multiple databases (i.e. perform distributed transactions), transmit large data sets (e.g. schema-conformant e-Documents) and perform searches across several databases. X-Road was designed with growth in mind, so can be scaled up as new e-services, with their various platforms, come online.

DEC layer

In addition to traditional records exchange methods offered by X-ROAD, the Document Exchange Centre (DEC) which functions through the X-Road is widely used by Estonia's public sector institutions; its operating principles are shown in the following figure (Figure 15).

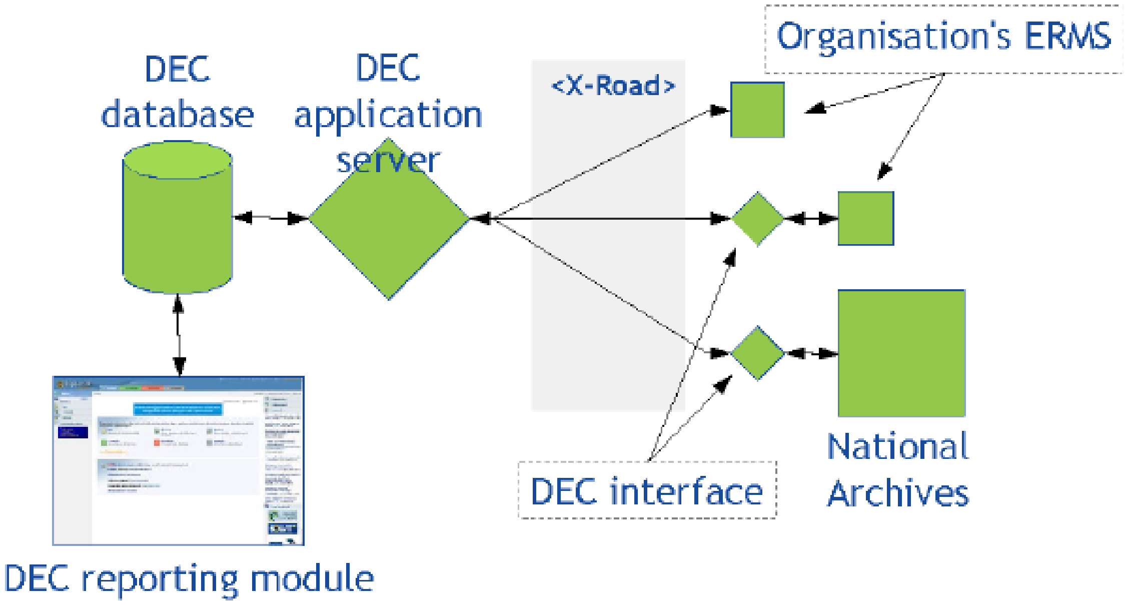


Figure 15: DEC Architecture

The goal of the DEC in the near future, to provide services that support the processing of records. Exchanging electronic records through the DEC is compulsory for all government authorities. In addition, more than 500 bodies and organisations have voluntarily joined the DEC (an actively updated list of the organisations is available at http://www.eesti.ee/portaal/dvk.asutused).

In order to use the DEC, each communication partner must have a DEC account and each organisation communicating with the DEC must have an X-Road security server for creating a secure connection. Technical interconnection with the DEC is possible through the DEC universal client interface offered by the Estonian Information System's Authority and the DEC Java API. In order to ensure problem-free records exchange, an organisation joins the DEC production environment only when its Electronic Record Management System (hereinafter ERMS) is completely prepared for receiving and sending records through the DEC. The DEC test environment must be used when testing the interface and the records exchange process.

Since the number of DEC users is constantly increasing, the ERMSs contact the DEC at least once daily to download the latest list of users. This allows for the automatic sending out of records: DEC is automatically appointed as the method of record-transferring given that the addressee is on the list of organisations that have joined the DEC.

Since the DEC data exchange takes place over the secure X-Road, the authentication and authorisation of the senders and recipients of records is done automatically with the help of the X-Road security servers. Citizens and companies can exchange records with organisations that have joined the DEC and monitor the course of the processing of the records through the mediation of the Official Records Infrastructure Service (ADIT), which has been created for the State Portal eesti.ee.

The e-invoices of private companies are transferred by the DEC to organisations through operators that handle private sector settlements or through a new service “Create an e-invoice” of the State Portal. The DEC can also be used for the purpose of exchanging records and the data there of between ERMSs and other organisational or inter-organisational information systems (for example, legislation is sent to Riigi Teataja for publication through the DEC).

DigiDoc layer

DigiDoc is a system that’s widely-used in Estonia for storing, sharing and electronically signing documents. Because electronic signatures carry the same legal weight as paper signatures in Estonia (see Legal Drivers section), a secure, easy-to-use platform is needed to give government institutions, businesses and private persons a way to perform electronic signing and transmit electronic documents.

After logging into the DigiDoc system with an ID card or Mobile ID, a user can upload any document, electronically sign it, and forward it to other parties for their signatures. Any type of file can be entered for signature – a word processing document, a photo or even an instant messaging chat. Voice recordings can be uploaded by phone.

The documents are stored in a unique folder for each user. Every time users log on, they see their own uploaded files and as well as any they have signed. DigiDoc utilizes the robust public key encryption of the Estonian ID card and Mobile-ID, meeting the EU’s strictest standards for security.

The system is heavily used in Estonia’s public sector, handling everything from court documents to municipal contracts. It’s also commonly used in the banking industry, though its popularity in all areas of business is growing rapidly.

E-Identification layer

In a nutshell, the e-Identification framework of Estonia consists of the following three complementary solutions (i) e-ID, (ii) Mobile-ID and (iii) STORK

(i) e-ID

e-ID is realized through a mandatory national card that is provided to each citizen and serves as the digital access card for all of Estonia’s secure e-services. The chip on the card carries embedded files which, using 2048-bit public key encryption, enable it to be used as definitive proof of ID in an electronic environment. Here are some examples of how the ID card is regularly used in Estonia (see identified domains):

- As a national ID card for legal travel within the EU for Estonian citizens
- As the national health insurance card
- As proof of identification when logging into bank accounts from a home computer
- As a pre-paid public transport ticket in Tallinn and Tartu

- For electronic signatures
- For e-voting
- For accessing government databases to check one's medical records, file taxes, etc.
- For picking up e-Prescriptions

(ii) Mobile-ID

Mobile-ID is service that allows a client to use a mobile phone as a form of secure electronic ID. Like the ID card, it can be used for accessing secure e-services and electronically signing documents, but has the advantage of not requiring a card reader. The system is based on a specialized Mobile-ID SIM card which the customer must request from the mobile phone operator. Private keys are stored on the mobile SIM card along with a small application for authentication and signing.

Here's how Mobile-ID would be used for logging into a secure site, for instance a bank account:

- The user clicks the "Log in with mobile ID" option on a supported website
- The phone beeps and displays a screen indicating that a connection is being made.
- The user is prompted to enter a mobile ID pin code into the phone.
- The screen on the phone disappears and the website is automatically reloaded with a logged in screen.

As smart phone technology becomes more widespread, having the Mobile-ID option will become increasingly handy, allowing the user to vote, for instance, via a phone's web browser.

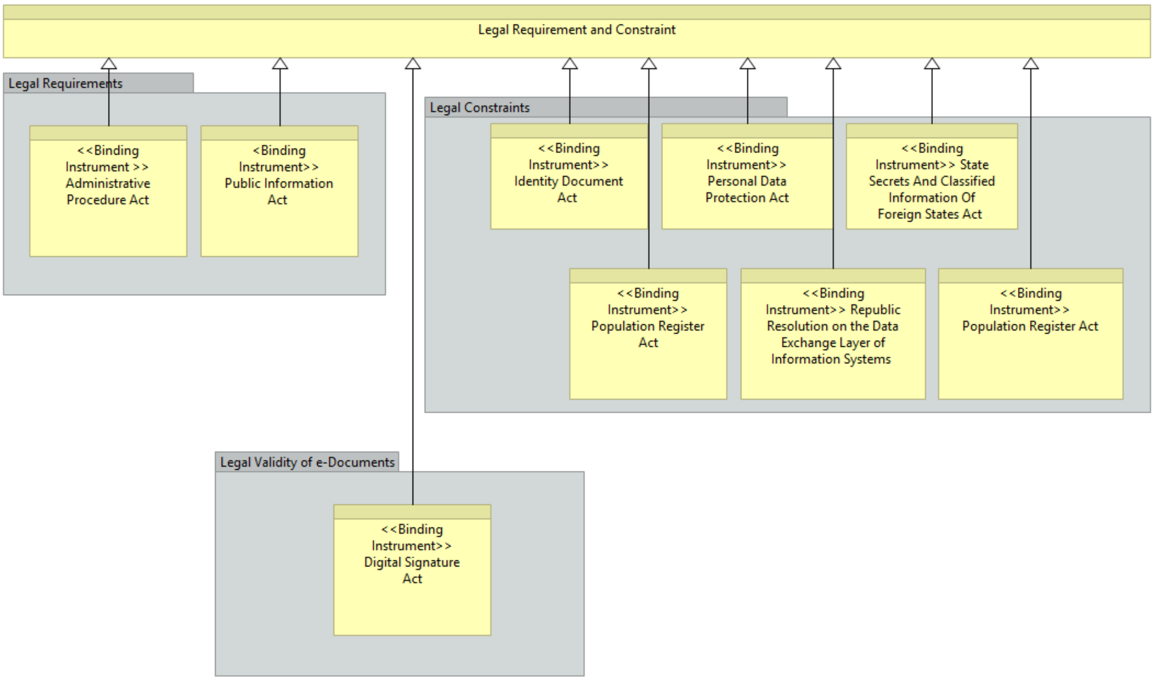
(iii) STORK

STORK [40] is not an Estonian project. It was the outcome of an EU Large Scale Pilot (LSP) project. The aim of the STORK project was to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. Cross-border user authentication for such e-relations was successfully applied and tested by the project by means of five pilot projects that were use existing government services in EU Member States. Estonia also takes part in the STORK2 LSP project.

I.2.1.3 Legal view

Estonia has developed a legal framework based mainly on the Administrative Procedure Act and the Public Information Act. Furthermore, several legal frameworks support e-Document processes; such as the Electronic signature

Act, the Identity Document Act etc. According to these Acts all e-Government processes can be digitized and practically paper-less. This increased the efficiency in the performance of administrative procedures. However, this paper-less approach is not only applicable in Government-to-Government (hereinafter G2G) processes but is generalized also in Government-to-Citizen (hereinafter G2C) processes.



Legal Requirement and Constraint
Legal Requirements
<<Binding Instrument >> Administrative Procedure Act
<Binding Instrument>> Public Information Act
Legal Constraints
<<Binding Instrument>> Identity Document Act
<<Binding Instrument>> Personal Data Protection Act
<<Binding Instrument>> State Secrets And Classified Information Of Foreign States Act
<<Binding Instrument>> Population Register Act
<<Binding Instrument>> Republic Resolution on the Data Exchange Layer of Information Systems
<<Binding Instrument>> Population Register Act
Legal Validity of e-Documents
<<Binding Instrument>> Digital Signature Act

Figure 16: Legal View for Estonia

ABB Legal Requirements

<<Legal Requirements>>
Binding Legal Requirements

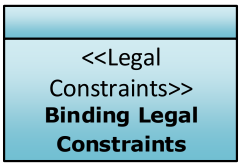
SBB: Binding Legal Requirements

As binding legal requirements we refer to Acts that regulate the usage of e-Documents. The following two Acts can be considered primary legal requirements for the Estonian case.

- **Administrative Procedure Act** [23], which equalizes electronic and written operations in administrative procedures and enables electronic interactions/delivery between citizens and administrative bodies.
- **Public Information Act** [41]**,** which provides the conditions of, procedure for and methods of accessing public information (including the procedure for

maintaining registers of records), the bases for establishing and managing databases and the supervision of the organisation of database management and the provision of access to information.

ABB Legal Constraints



SBB: Binding Legal Constraints

There are several legal requirements that accompany the legal drivers. These requirements are summarized below:

- **Identity Document Act** [42] which establishes an identity document requirement and regulates the issue of identity documents to Estonian citizens and aliens by the Republic of Estonia. According to the Act, each Estonian citizen staying (residing) permanently in Estonia shall hold an identity card. Also, an alien staying (residing) permanently in Estonia on the basis of a valid residence permit shall hold an identity card. Each identity card [43] contains two certificates: one for authentication and one for electronic signing. There are also two associated private keys, protected by two separate PIN codes, on the card. The certificates contain no restrictions of use: they are by nature universal and meant to be used in any form of communications, whether between private persons, organizations or the card holder and government. Therefore, any Estonian citizen is enabled to sign e-Documents and validate them through specific utilities that are provided.

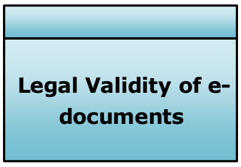
- **Personal Data Protection Act** [44], which provides the conditions and procedure for processing personal data, the procedure for state supervision over the processing of personal data and the liability for violation of the personal data processing requirements.

- **National Archives Act** [45], which states that the archival processing and transfer of digital documents is basically not different from ordinary archival processing procedure. Similarly to the non-electronic procedure, an inventory, a compilation of archives description and other documentation, arrangement of records, preparing these for long-term preservation requirements and transfer to an institution or public archives are required. Only the instruments employed are different. The institutions must act in accordance with the National Archives' guidelines Archives management requirements for digital records (in Estonian) (version 1.0. 17.12.2008) and Transfer of records (in Estonian) when conducting archival processing of digital documents.

- **State Secrets And Classified Information Of Foreign States Act** [46]. The purpose of this act is to ensure the security and foreign relations of the Republic of Estonia, protecting state secrets and classified information of foreign states from disclosure and becoming accessible to persons who have not been granted access to such information. According to this act, the exchange of e-Documents should contain specific classification meta-data.

- **Population Register Act** [47], which provides the conditions for introduction and maintenance of the population register, processing of data and access to data in the population register. The purpose of this Act is to ensure the collection of main personal data of the subjects of the population register in a single database for the performance of functions of the state and local governments. At a first glance this may not be highly correlated to the e-Documents processes, however it is. Based on this act and the combination with the Identity Document Act, for each Estonian citizen, a record in a central repository exists that contains his/her public metadata along with the public key of the certificates that are included in the e-ID. This feature practically, provides the capability of routing signed e-Documents to any citizen by any citizen; thus it could be argued that is practically an enabler as far as the adoption of e-Documents is concerned**.** It does so by providing a lookup service for any endpoint. Lookup queries are performed on top of name, email and idcard-number. The routed e-Document is persisted in a Governmental Cloud temporarily until it is being fetched/claimed by the routing endpoint.

- **Government of the Republic Resolution on the Data Exchange Layer of Information Systems** [48]. The resolution sets requirements for the data exchange layer of information systems, its use and management. This is more relevant to the structured e-Documents.



Specialisation: Legal Validity of e-Documents

The legal validity of e-Documents relies on the Electronic signature Act [24] (DSA). According to this legislation, an electronic signature is equal to a hand-written signature. We consider this act as foundational since all Estonian authorities are obliged to accept digitally signed documents. The Act was introduced on 8-March 2000 and is amended 6 times until 8-January 2004. The Act provides the necessary conditions for using electronic signatures and the procedure for exercising supervision over the provision of certification services and time-stamping services. Regarding the Act's legal consequences the Act states that:

- An electronic signature has the same legal validity as a hand-written signature under specific consequences.

- The giving of an electronic signature without the consent of the holder of the corresponding certificate is deemed to be proved if the certificate holder proves circumstances which existed and due to which it may be presumed that the signature was given without his or her consent.

The validity of e-Documents is highly correlated with the validity of the Certificates that are used in order to sign the documents. The Certificates that may be used may derive by any Certificate Service Provider (CSP) that operates under the DSA [43]. DSA regulates the work of CSPs in Estonia, setting forth requirements to them and regulating their operation and supervision. CSPs may only be legal entities with a regulated minimum share capital, they must be entered in the National Certificate Service Provider Registry and must carry out an annual audit to ensure organization and system reliability. CSPs must also have liability insurance to safeguard against compensating faults made while providing the service.

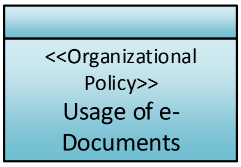
It is important to note that according to DSA, CSPs certify only real persons identifiable by name and an identifier – issuing certificates to pseudonyms is not currently covered by DSA. This has been discussed in the parliament during the law adoption process, but was considered to be an additional unnecessary risk and so far, no need for this has been seen.

Time stamp validity

DSA also regulates the work of Time stamp Service Providers (hereinafter TSPs) and the comparison of time stamps between TSPs. The requirements to service providers are generally the same as those to CSPs. According to DSA, a time stamp is simply a data unit that proves that certain data existed at a certain moment. DSA does not define time stamps in more detail, but states that they must be bound to the time stamped data and issued in such a way that it would be impossible to change the times tamped data without invalidating the time stamp.

I.2.1.4 Organizational view

ABB- Organizational Policy



SBB: Usage of e-Documents in administrative processes

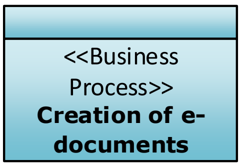
We can differentiate the usage of e-Documents in Estonia in Government-to-Government and Government-to-Citizen. Government-to-Government may refer to exchange of fully structured documents (using the X-ROAD system as a substrate) or any type of electronic document (using the Document Exchange Center). On the other hand, the Government-to-Citizen processes rely on documents that may be automatically generated by web-forms or by user-defined documents that one of the two parties selects to upload in an arbitrary way. Every citizen registers an email, which is used for asynchronous communication. Each upload is accompanied by a respective notification. The administrative processes where X-Road, eDoc and DigiDoc are used are grouped by the Estonian government in the following 11 domains:

- Population-Civil Record registries – individuals' addresses
- Tax board: e-Documents for tax debts, declarations
- e-Health: e-Documents for personal health data / records, doctors' licenses, prescriptions issued, health insurance cover
- Social insurance registries: e-Documents for individuals' benefits and claims
- Business registries: e-Documents for representation rights and reports
- Land registries: e-Documents for address data
- e-Police: e-Documents for traffic violations, missing persons and fugitives
- Vehicle and driver registries: licences, traffic insurance coverage
- Educational registries: e-Documents for educational records
- Unemployment data: e-Documents for benefits and claims
- Migration board

The usage of e-Documents is backed by the Digital Signature Act according to which the usage of electronic signatures includes:

- In relations in private law, electronic signatures shall be used according to agreement between the parties.
- In relations in public law, electronic signatures shall be used pursuant to this Act and legislation issued on the basis thereof.
- State and local government agencies, legal persons in public law, and persons in private law performing public law functions are required to provide access through the public data communication network to information concerning the possibilities and procedure for using electronic signatures in communication with such agencies and persons.

ABB- Business Process



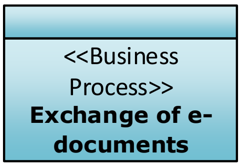
SBB: Creation of e-Documents

Taking under consideration the IT ecosystem in Estonia we will differentiate the e-Documents' creation process for the two basic components that are used; namely the DigiDoc and the DEC. Regarding the DigiDoc, e-Documents can be created using two different ways:

- By using existing electronic documents (word, pdf, image, txt) accompanied by metadata that are bound to the format of the document;
- By scanning paper-documents, accompanied by metadata that are assigned during the digitisation procedure;

Regarding DEC, the creation of structured e-Documents is based on a set of elements for each document type, which are also used to develop the record templates used in Electronic Record Management Systems (hereinafter ERMSs). The elements of e-Documents and the description of document types are discussed in the regulation of the Government of the Republic on the Common Principles of Administrative and Records Management Procedures. Among other things, the regulation provides for the confirmation of the set of elements for a record type through development of a data description. The elements of one record type are established in the national standard EVS 882-1:2006. The elements of a record type can partially coincide with the record metadata elements entered in the ERMS. In this case, the ERMS should be able to transfer the values from the draft record to the metadata or the other way around.

Furthermore, during the creation process a certificate that meets the requirements set forth in the Digital Signatures Act is used when electronically signing records. However, the signature is not an obligatory element for every record and may be absent if legislation does not require its presence in the case of the type of record at hand and if the record has been captured into the ERMS by an authenticated and authorised user and is permanently linked to or related to the necessary metadata. For example, a signature is not necessary in the case of informative letters (notices, etc.). If necessary, records will be confirmed with an electronic seal. Additionally, it is advisable to create digital records with a long retention period (more than 10 years) in formats suitable for long term preservation.



SBB: Exchange of e-Documents

The exchange of e-Documents can be separated in two different categories:

- **User-based exchanges** where a user (Citizen or civil servant) performs the exchange procedure outside X-ROAD/DEC. This procedure is realized through DigiDoc and it includes
  - The selection of the routing endpoint
  - The creation of the container
  - The (possible) signing of the payload
  - The (possible) encryption of the payload

- **Systemic exchanges** where specific bridges are already established between two administrative organizations. X-ROAD protocol and DEC platform play a significant role on this type of exchange

In the User-based exchanges, a user selects the documents that s/he wishes to package in a container. After the container creation, the user selects the routing endpoint. In Estonia each candidate routing endpoint (Citizen, Civil Servant or Organization) is registered in a central registry along with some lookup metadata. After the selection of the endpoint, the sender chooses to sign and/or encrypt the e-Document before routing.

In Systemic Exchanges, exchanged documents can be in any format and size. The document will be put in a so-called DEC envelope (see DEC container section above), to which the data of the sender and the receiver will be attached. DEC does not read the content of the file, only forwards it to the receiving information system. This enables to send files both in machine-readable formats (e.g. XML) and in all other formats (PDF, DOC, etc.).

Records are transferred in SOAP envelopes with XML containers ("envelopes" of records) each of which, in turn, contains a record and an extract of its metadata. The transfer of a standard metadata set facilitates the capturing and registration of the records in the recipient's system, since the necessary metadata can be populated automatically.

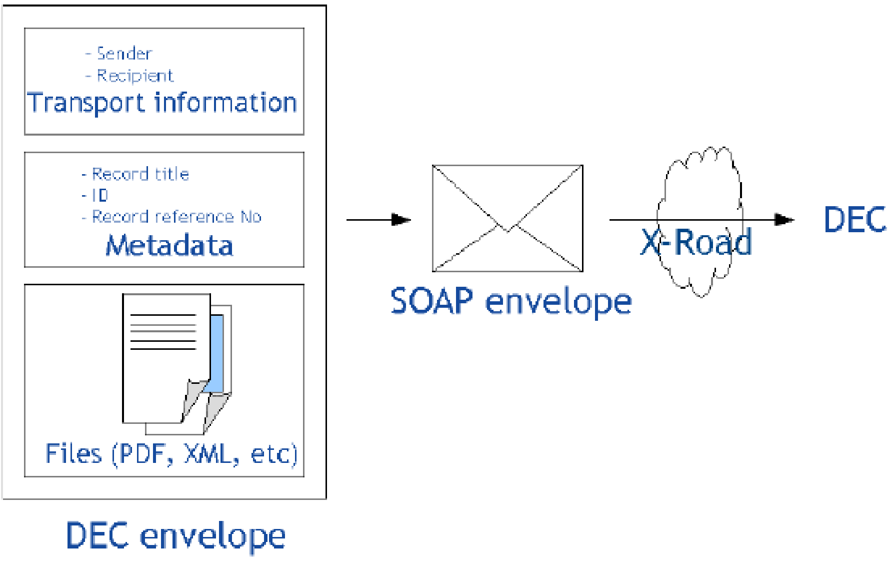


Figure 17: e-Document transfer through DEC

Instead of passing on the records that arrive at the DEC central server, the server waits for the communication partner itself to ask for the newly arrived records. This "pull pattern" was preferred over "push patterns" (e.g. email).

Upon the arrival of the records, the recipient's system returns the appropriate confirmation. Furthermore, authorised employees of an organisation that has joined the DEC can use the DEC reporting module for searching and viewing records sent and received by the organisation, grouping the records on the basis of various criteria (e.g. sending time, status, sender, and recipient) and preparing reports based on this information.

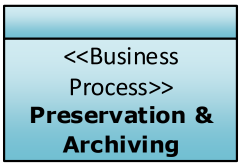
SBB: Access to e-Documents

The access to the e-Documents is provided by the following systems (based on the type of the exchange):

- **Digidoc Portal** which is used mainly in Citizen-to-Government and Citizen-to-Citizen e-Document exchanges
- **DEC Portal** which is used on Government-to-Government exchanges between two X-ROAD endpoints (which pre-assumes that a system is already interconnected using the X-ROAD protocol)

For the first case there is no system-level mechanism of controlling the access to the documents since any exchange is personalized; thus the two parties maintain the full responsibility regarding the disclosure of information of the transferred document.

In the DEC case, any e-Document is accompanied by specific metadata (Access Restriction Identifiers) that defines Access Policies. These metadata are interpretable by DEC; therefore access restrictions and time-validity of these restrictions can be centrally applied.



SBB: Preservation & Archiving

All e-Documents in an ERMS must be assigned a retention period. Retention periods are primarily established on the basis of the requirements set forth in legislation which, in certain circumstances, can also be obligatory for the private sector. If the retention period of the records of a class has not been provided in legislation, the retention period will be determined by the head of the organisation upon the approval of the list of record classes.

Although records in ERMSs are generally assigned the retention period of the appropriate class or file automatically (i.e. through inheritance), it must also be possible to set retention periods manually. Furthermore, an ERMS must allow users to determine events that trigger the calculation of the retention period or serve as the end points for retention periods. Retention period management is supported by the multi-level retention and disposition schedules described in MoReq2.

In Estonia, public archives conduct appraisals to determine which records have archival value and will therefore be retained permanently. Records with archival value must be transferred to public archives and constitute a part of the national cultural heritage. An ERMS must provide an option for marking the classes or files on which the public archives have rendered their appraisal decisions and identifying classes or files as having archival value or being subject to disposition and destruction pursuant to the usual procedure. For this purpose, the information concerning appraisal decisions is entered into the metadata of a class or a file. The ERMS must preclude the destruction of files or classes and the records belonging thereto if they have been identified as having archival value, regardless of the initial retention periods assigned to these files or classes.

There are two methods for retaining digital records and the distinction between the methods is mainly organisational. Firstly, retaining records in an ERMS, which may be the only place where records with short retention periods are stored, and secondly, the retention of digital records in an archive management system after their disposition from the ERMS. An archive management system can be a system maintained by an organisation, a service provider or public archives.

The ERMS may have other archival functionalities in addition to the functionality of managing retention periods. Estonian legislation does not provide requirements for digital archival software, although the OAIS (Open Archival Information System) model is usually followed in terms of architecture and functionality in accordance with the standard ISO 14721:2003 "Space data and information transfer systems. Open archival information system. Reference model". However, there is a specific tool called Universal Archiving Module that can be used by organizations in order to convert the archives in proper format and provide the appropriate metadata.

Records that have been created or received in the course of the performance of public duties and have been determined to possess archival value as a result of an appraisal are transferred to the National Archives (except when provided otherwise by law). According to the Archives Act that came into force in 2012, an organisation can transfer such records as soon as they are no longer necessary for the performance of its duties and has to transfer the records no later than 10 years after creating or receiving them. The National Archives are using the software module "Safety Deposit Box 4" (SDB4)**Invalid source specified.**.

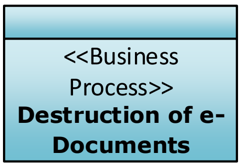
In addition to records with archival value, public institutions can use the service of the National Archives to store digital records with no archival value if their retention period is longer than 10 years. The retention of digital records with shorter retention periods must be ensured by the institution's own ERMS. Records must be transferred to the National Archives in accordance with the guidelines provided by the National Archives.

The National Archives has approved a list of formats that are suitable for the long term retention of digital records with archival value: XML (Extensible Markup Language); TXT; PDF (Portable Document Format), PDF/A format recommended; TIFF (Tagged Image File Format); PNG (Public Network Graphics); BWF (The Broadcast Wave

Format); AIFF (Audio Interchange File Format); decompressed video; video formats created with the video compression method MPEG-2. As of 1 January 2013, public sector institutions will be obligated to create digital records with long retention periods (in excess of 10 years) in formats that are suitable for long-term retention. This requirement ensures that records with a long retention period are created using file formats suitable for long term preservation and can be transferred to the National Archives securely and without additional processing.

In order to facilitate the transfer of digital records with archival value to the archives, the National Archives have created a software tool: the Universal Archiving Module (UAM). UAM enables an archival scheme to be created using the classification scheme of an ERMS or its structure to be modified (as an example to merge classes). The records are exported from the ERMS to the UAM where they are (1) arranged and (2) described in accordance with the archival description rules. In the course of the arrangement, UAM enables the migration of records into file formats suitable for long term preservation (if necessary), etc. During the archival description phase, the archival description of the material is semi-automatically created based on the existing records management metadata.

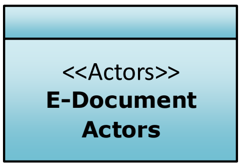
In order to enable the use of the UAM, the ERMS must be capable of exporting data in the XML format; additionally, a mapping table in XSL format has to be created to transform the export into the XML format with semantics and structure supported by UAM. The UAM XML format is defined by an XML Schema (XSD) and available from the National Archives' website.



SBB: Destruction of e-Documents

In the public sector, e-Documents cannot be destroyed before the National Archives have issued an appraisal report regarding the records. The destruction of records (as well as their disposition and transfer) must take place in a controlled manner and must be duly documented. A certain segment of metadata, or a metadata stub, is retained after the destruction of records. At the same time, an ERMS is responsible for ensuring the complete and irreversible deletion of the records and creating and retaining sufficient documentation on the destruction of the records.

ABB-Actors



SBB: e-Document Actors

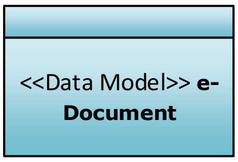
The main actors that play an active role in e-Document exchange are Citizens and members of the Governments and the Administrations. The big difference between them is that the Citizens are using only one interaction modality (i.e. DigiDoc) while the Administration members interact with several modalities. These modalities may include legacy systems that are interconnected through X-ROAD or centralized (cloud) solutions such as DEC.

It is worth mentioning that in Estonia any citizen can send a signed and encrypted e-Document to another citizen directly through the usage of the national registry (i.e. an LDAP repository that contains all citizens) and the DigiDoc component (analysed more thoroughly below). However, through the same component (DigiDoc) an exchange between a citizen and a governmental agency can also be realized (G2C processes). On the other hand, the usage of DEC can facilitate the communication only between governmental agencies (G2G processes). This is mainly because DEC has strong technical prerequisites that have to be met in order to join its ecosystem (i.e. security on-boarding and data harmonization procedures).

Another Actor is the ERMS Archiver which is responsible for the operation of the Universal Archiving Module. The product of this tool may be forwarded to the National Archives (if the output is of significant archival value). Therefore the National Archiver is also an Actor. Moreover, after the creation of an e-Document someone must evaluate the document’s importance as far the national security is concerned (or the organization’s security). This evaluation leads to the creation of specific e-Document Access Policies. Therefore, this role could be the Access Policy Administrator.

I.2.1.5 Semantic view

ABB-Data Model



SBB: e-Document

Regarding the tem document, as in the case with many other languages, the main difficulties in the Estonian environment have arisen from translating the terms record and document [3]. Estonia is one of the cultures where a term similar to the English word document (in Estonian: dokument) has traditionally been used to refer to the concept denoted in English by the term record. The pronunciation and the spelling of the English word document are practically the same as that of the Estonian word, while the English term is also connected to the concept of documenting something. So far, the word dokument has been used in the Estonian translations of texts pertaining to records and archive management as the equivalent of both English terms (record and document).

However, a document is not the same as a record. Due to this, the identical translation of two of the main terms related to records management has given rise to misunderstandings and questions in the past; in the case of the MoReq2 [3] translation, the use of the same Estonian word for both terms would occasionally make the text completely incomprehensible.

The records and archive management experts who participated in the discussions on MoReq2 terminology came to the conclusion that the definition of **the term record as presented in the ISO 15489-1 standard as well as MoReq2 overlaps in essence with the Estonian definition of dokument as presented in Estonia's Archives Act, according to which a dokument is "information recorded on any medium, which is created or received in the course of the activities of an agency or person, and the content, form and structure of which is sufficient to provide evidence of facts or activities."** Since this definition has been in use ever since the Archives Act was first published in 1998 and is widely recognised by Estonian experts in the field, it was determined that dokument should be used as the equivalent of record in Estonian and that a new translation should be found for the English term document.

The experts considered it important to describe the way **documents** (Estonian teavikud) are related to **information** (Estonian teave) and **records** (Estonian dokumendid), which is visualised in the figure below: some information is recorded, forming documents; some documents are declared as records that have to be duly retained for as long as is necessary for use as a source of information or as evidence. Memory institutions permanently preserve records (but also documents), which have informational or evidential value that is not reduced even in a very long term and which are also expected to interest future historians.

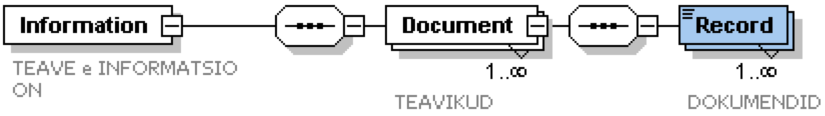
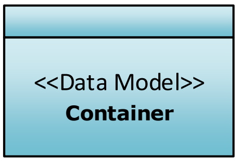


Figure 18: Record / Document / Information

For the sake of harmonic presentation of our desktop research, the term e-Document is used to represent the most granular exchangeable entity which in Estonia is addressed as record.

However, in Estonia, when referring to encapsulating entities of e-Documents (entities that wrap e-Documents), this results in an ambiguity, which will be explained in the next section.



SBB: Container

The term "Container" is used to model an entity that wraps many instances of e-Documents. However, this term may lead to misunderstanding. On the one hand, as far as the DigiDoc component is concerned, Container is used to model a serialization format that is used in order to bundle several e-Documents. This container is addressed as a BDOC container.

The BDOC file format is based on ASiC [28] standard, which is in turn profiled by the ASiC Basic Profile. The latter foresees ODF-type packaging specified in OpenDocument standard of OASIS. BDOC packaging is a ASiC-E XAdES type ZIP container with the following requirements followed:

- **mimetype file**. The file "mimetype" shall be present in uncompressed form and formed as described in clause A.1 of the ASiC standard. The content must be: **application/vnd.etsi.asic-e+zip**
- **manifest file.** The file "manifest.xml" shall be present in directory META-INF/ and contain list of all directories and files with their types present in the container as described in section 3.2 of the OpenDocument [49] standard.

The following sample BDOC file contains single embedded data file and one signature.

BDOC file structure

- **document.doc**

- mimetype
- META-INF/manifest.xml
- META-INF/signatures1.xml

Content of file “mimetype”

- **application/vnd.etsi.asic-e+zip**

Content of file “META-INF/manifest.xml”

```
<?xml version="1.0" encoding="utf-8"?>
<manifest:manifest
xmlns:manifest="urn:oasis:names:tc:opendocument:xmlns:manifest:1.0">
<manifest:file-entry manifest:media-type="application/vnd.etsi.asic-e+zip"
manifest:full-path="/" />
<manifest:file-entry manifest:media-type="application/msword"
manifest:full-path="document.doc" />
</manifest:manifest>
```

Content of file “META-INF/signatures1.xml”

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<asic:XAdESSignatures xmlns:asic="http://uri.etsi.org/02918/v1.2.1#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#">
<ds:Signature Id="S0">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-
c14n11"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha224"/>
<ds:Reference Id="S0-RefId0" URI="document.doc">
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>5UyKB9ht94y6CZNvLdO1C7Z3MXaYc2Qol3Dt3Qp4Ajg=
</ds:DigestValue>
</ds:Reference>
…
```

On the other hand, in the DEC system the container is an aggregation of e-Documents serialized in XML accompanied by a set of metadata that are relevant to the exchange. Any electronic document can be Base64-encoded and embedded to the DEC container.

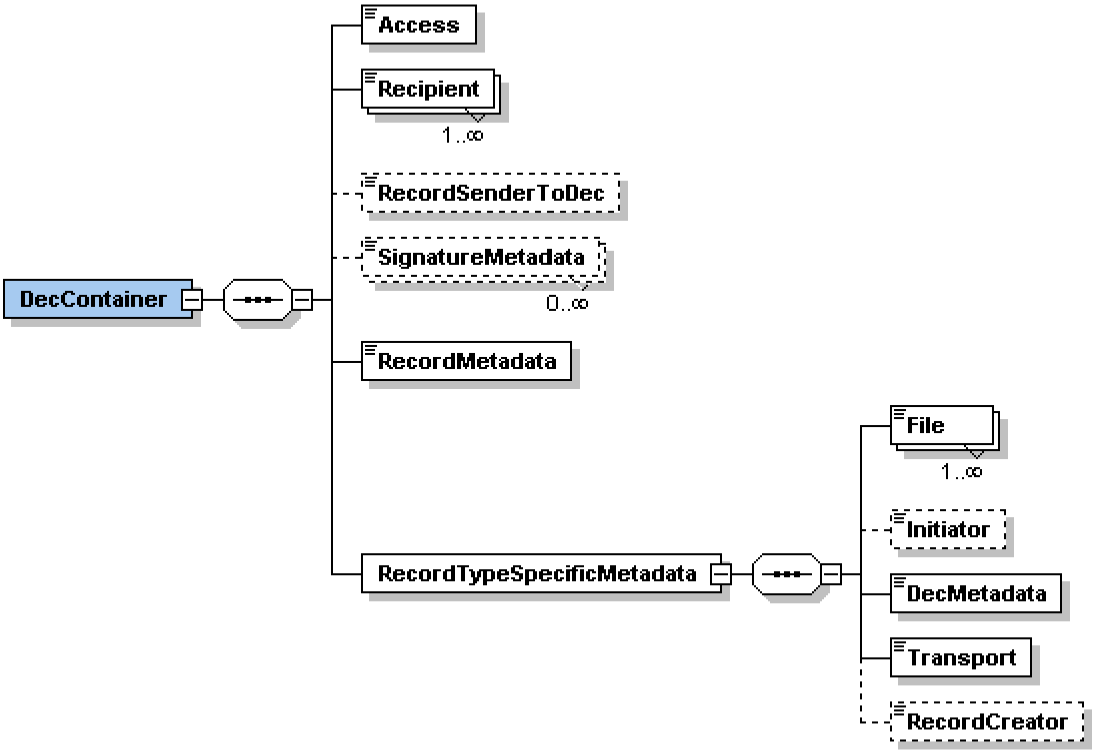


Figure 19: DEC Container

Therefore, there are two types of e-Documents' encapsulation.

ABB- Metadata

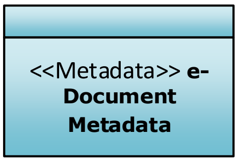
Estonia defines the list of metadata designed to ensure that the documents (and information in them) can be easily switched between different organizations and computer systems, as well as to ensure that they can be trusted for a longer period of time. The agreement on the common list of metadata aim at creating user-friendly e-public service, paperless administration and digital archiving [50].

The list of mandatory and optional metadata was built in accordance with Archives Act [45], under the assumption that the exchange infrastructure is DEC (Document Exchange Center) and X-Road. With regard to the metadata of e-Documents, the source document currently in force in Estonia is "Dokumendihalduse metaandmete loend" (Records Management Metadata Set) [50], the first version of which was issued by the Government Office in 2006. The original set was compiled on the basis of the standards EVS-ISO 15489-1 and EVS-ISO 23081-1 as well as foreign and international metadata models. The list differentiates between **13 metadata blocks**:

1. Metadata about mandates (regulatory requirements providing mandates for record creation);
2. Metadata about functions;
3. Metadata about classification schemes;
4. Metadata about classification units (class, sub-class, file);
5. Metadata about records;
6. Metadata about components (computer files);
7. Metadata about access controls;
8. Metadata about activities and transactions (e.g. registration of the record, opening of the file);
9. Metadata about the organisation (description of the organisation that created the records);
10. Metadata about groups/sections (e.g. department, division, working group);
11. Metadata about positions/roles (e.g. manager, specialist);
12. Metadata about agents;
13. Address metadata.

The aforementioned set contains 93 different elements and 60 element qualifiers, thereby providing a sufficient semantic base for the description of the most important data retained in ERMSs. The elements have been supplemented with references to equivalent elements found in foreign or international metadata models (including MoReq). The list is altered when required: when legislation is amended, new standards are adopted or a practical need for change arises. During the revision of the metadata set in 2012, the metadata elements used in the records exchange via DEC and for the disclosure of registers of records will be added together with new references to equivalent elements, and the textual part of the set will be updated.

The Records Management Metadata Set has been one of the source materials used for procuring and developing ERMSs in Estonia since 2006. The National Archives have used it as the basis for creating a list of metadata necessary for archiving and developing a universal archival module (UAM).



SBB: e-Document Metadata

The following table summarizes the metadata used by the DEC system during e-Document exchange.

Table 3: DEC Metadata

Title	Type	Explanation
DecContainer	xs:complexType	
Access	xs:complexType	Access to the document metadata
AccessRestriction	xs:complexType	Imposed restrictions on access to the document description
RestrictionBeginDate	xs:date	Date of access restriction signs (signs of the date of preparation)
RestrictionBasis	xs:string	Legislation under which the limit is set
RestrictionInvalidSince	xs:date	Restriction of access to the document Date of expiry
InformationOwner	xs:string	Access restriction (primary) introduced the name
RestrictionEndDate	xs:date	Maximum date of termination of access restriction
RestrictionEndEvent	xs:string	The event which takes place a maximum limit expires before the final deadline
RestrictionIdentifier	xs:string	Identification of the classification of restricted access
AccessConditionsCode	tns:AccessConditionType	The document given access to a description of the condition
Recipient	xs:complexType	The addressee details
Person	tns:PersonType	Recipient of personal data
RecipientRecordOriginalIdentifier	xs:string	Document reference links that points to the location of the recipient of the document in the system
ContactData	tns:ContactDataType	Recipient contact information
MessageForRecipient	xs:string	The document accompanying commentary, corecipient of the letter
Organization	tns:OrganisationType	Recipient Organization Profile
RecipientRecordGuid	tns:GuidType	Related document the unique identifier of the recipient's system
RecordSenderToDec	xs:complexType	Document of the sender

Title	Type	Explanation
ContactData	tns:ContactDataType	The sender's contact details
Person	tns:PersonType	The identity of the sender
Organization	tns:OrganisationType	Recipient Organization Profile
SignatureMetadata	xs:complexType	Signing the document metadata
SignatureVerificationDate	xs:dateTime	Date and time of signature verification
Sign	xs:string	The document signer
SignatureType	xs:string	The signature of the document type
Verified	xs:string	The validity of the signature confirmation
RecordMetadata	xs:complexType	Expelled document metadata
RecordDateRegistered	xs:dateTime	Document the date and time of the transmitter system
RecordType	xs:string	Document type designation
ReplyDueDate	xs:date	The document accompanying the transmission of the response deadline
RecordOriginalIdentifier	xs:string	Document link that points to the location of the sender of the document in the system
RecordGuid	tns:GuidType	Unique identifier of the document
RecordTitle	xs:string	Document title
RecordLanguage	xs:string	The contents of the document representation language
RecordAbstract	xs:string	Brief presentation of the contents of the document in free text
RecordTypeSpecificMetadata	xs:complexType	RIHA described the type of the document metadata
File	xs:complexType	File metadata
RecordMainComponent	xs:boolean	Indicates whether the file is the principal document
File GUID	tns:GuidType	File a unique identifier

Title	Type	Explanation
FileSize	xs:integer	Document of data file to the volume of the component part
ZipBase64Content	xs:string	Wipe the ZIP file and put the contents of Base64 encoding
FileName	xs:string	Document or component part of the file name
Initiator	xs:complexType	Details of the source document
Organization	tns:OrganisationType	The initiator of the organization's data
InitiatorRecordOriginalIdentifier	xs:string	Source document five
ContactData	tns:ContactDataType	The initiator of contact information
Person	tns:PersonType	The initiator of personal data
InitiatorRecordDate	xs:dateTime	Document the date and time of departure
DecMetadata	xs:complexType	DEC's automatically added to the metadata
DecReceiptDate	xs:dateTime	DVK into the document the date and time of the arrival
Decide	xs:integer	DEC document a unique identifier
DecFolder	xs:string	DEC document in a folder
Transport	xs:complexType	Document addressing DVKs descriptive data
DecRecipient	xs:complexType	Document the recipient organization or individual Departments
OrganisationCode	xs:string	A legal person registration code
StructuralUnit	xs:string	A legal person under / Departments
PersonalIdCode	xs:string	Personal identification Code
DecSender	xs:complexType	Document sending organization or individual Departments
PersonalIdCode	xs:string	Personal Identification code
OrganisationCode	xs:string	A legal person registration code
StructuralUnit	xs:string	A legal person under / Departments

Title	Type	Explanation
RecordCreator	xs:complexType	The originating authority / responsibility data
ContactData	tns:ContactDataType	Compiled contact details
Organization	tns:OrganisationType	An organisational Data
Person	tns:PersonType	Compiled personal data

Archive Metadata

Beyond DEC's metadata, the full set of archiving metadata are provided below

Table 4: Archive Metadata

	Item Name	Mandatory	Condition
The classification scheme			
1	Classification Scheme Identifier	Y	
2	Classification Scheme Name	Y	
3	Responsible for the Classification Scheme	Y	
4	Date of Classification Scheme	Y	
4.1	The date of opening of the classification scheme	Y	Y, where the body is arhiivimoodustaja
4.2	Classification Scheme DATE	N	
4.3	The classification scheme change date	N	

	Item Name	Mandator y	Condition
4.4	The date of closing of the classification scheme	N	
5	Description Classification Scheme	N	
Liigitusüksus			
6	CLASSIFICATION identifier	Y	
7	CLASSIFICATION Type	Y	
8	CLASSIFICATION five	Y	
9	CLASSIFICATION Title	Y	
10	CLASSIFICATION description	N	arhiivimoodustajatel Y function level
11	CLASSIFICATION keyword	N	
11.1	Thesaurus	N	
12	CLASSIFICATION Date	Y	
12.1	CLASSIFICATION creation date	Y	
12.2	CLASSIFICATION date of opening	Y	
12.3	CLASSIFICATION date of closing	N	Y if liigitusüksus is closed
12.4	CLASSIFICATION archives of the delivery date	N	Y, if a file is open or in the case of the archives of the

	Item Name	Mandator y	Condition
12.5	CLASSIFICATION preserves of the delivery date	N	Y, if a file is to maintain a thing or transferred
12.6	CLASSIFICATION date of destruction	N	Y, after the destruction of the file or from the
13	CLASSIFICATION status	N	
14	Responsibility for classification units	N	
15	CLASSIFICATION Location	N	
16	The retention	Y	
16.1	Retention Period start date	N	
16.2	Retention Launcher	Y	Permanent retention of N
16.3	The duration of the retention	Y	
16.4	Retention period end date	N	
17	An appraisal	N	
17.1	Reference to the evalutaion decisions	Y	if there is an appraisal
17.2	The date of the assessment	Y	if there is an appraisal
17.3	the archival value notation	Y	if there is an appraisal
18	Disposition Schedule	N	

	Item Name	Mandator y	Condition
18.1	Disposition Schedule step description of the activity	Y	if the allocation schedule for implementing the
18.2	Disposition Schedule stage of maturity	N	
18.3	Disposition Schedule stage Launcher	N	
18.4	Message	N	
19	Power	N	Y, where the body is arhiivimoodustaja
19.1	Authorization Type	N	
19.2	Authorization Name	N	
19.3	Authorization Reference	N	
19.4	Mandate Description	N	
Document			
20	Document identifier	Y	
21	Document Type	Y	
22	Document Reference	Y	
23	Document liigitusüksus	N	
24	Document process step	Y	
25	Document Status stage of procedure	N	
26	Document Title	Y	
27	Document Gist	N	

	Item Name	Mandator y	Condition
28	Document keyword	N	
28.1	Thesaurus	N	
29	Document Language	N	
30	Document Date	Y	
30.1	Document creation date	Y	
30.2	Document the date of registration	Y	
30.3	Document date of separation	N	
30.4	Date of receipt of the document	N	
30.5	Document the date of dispatch	N	
30.6	Document deadline of compliance	N	
30.7	Date of adoption of the document	N	
31	Location	N	
32	Recording Type	N	
33	Document the organization's external context	N	
33.1	Document by an external party	Y	if the document has an outside party
33.2	Document the role of an external party	Y	if the document has an outside party
33.3	Link Link	N	

	Item Name	Mandatory	Condition
33.4	A non-party document identifier	N	
33.5	External party Date of document	N	
33.6	Document transmission method	N	
33.7	Message	N	
34	Document Extras	N	
File			
35	File identifier	Y	
36	File Name	Y	
37	File Format	Y	
37.1	Name of the file format	Y	
37.2	The file format version	N	
38	File size	N	
39	Stability	Y	
39.1	Value	Y	
39.2	Algorithm	Y	
39.3	Date of establishment	Y	
40	Software	N	
40.1	Software Name	Y	when the element is used
40.2	Software Version	N	
41	Encoding	N	

	Item Name	Mandatory	Condition
42	Purpose of use	N	
Access			
43	Conditions of access identifier	Y	
44	An indication of the conditions of access	Y	
45	Access Restriction	N	Y if the conditions of access is not an indication of the "public"
45.1	Restriction Identifier	Y	if the conditions of access is not an indication of the "public"
45.2	Beginning restriction	Y	if the conditions of access is not an indication of the "public"
45.3	Restriction Expiraton	Y	if the conditions of access is not an indication of the "public"
45.4	Duration Of Restriction	N	
45.5	Basic restriction	Y	if the conditions of access is not an indication of the "public"
45.6	Restriction closing event	N	
45.7	The restriction was invalid as	N	Y after the expiry of the limitation as Conditions of access is not an indication of the "public"
45.8	Holders of information	Y	if the conditions of access is not an indication of the "public"
46	Intellectual property	N	
46.1	Protection of intellectual property notation	N	

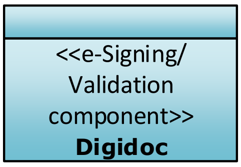
	Item Name	Mandatory	Condition
46.2	Term of protection of intellectual property	Y	if the document is the intellectual property
46.3	Intellectual property owner	Y	if the document is the intellectual property
47	Reproduction prohibited	N	
The body and the person			
48	Person identifier	Y	
49	Name of Person	Y	
50	Person Type	Y	
51	Registration Code	N	N, where the person is a legal person in Estonia
52	Privacy Code	N	
53	Legal Status	N	
54	Job Title	N	
55	Country	N	
56	County	N	
57	Local Government Unit	N	
58	Settlement or Administrative unit	N	
59	Small Spot	N	
60	Land unit	N	
61	Road Surface	N	
62	Address Number	N	

	Item Name	Mandatory	Condition
63	The number of components of the building	N	
64	Postcode	N	
65	Phone Number	N	
66	Faksininumber	N	
67	E-mail Address	N	
68	Web Page	N	
69	IM Address	N	
Activity			
70	Activity Identifier	Y	
71	Type of business	Y	
72	Performer	Y	
72.1	Performer Name	Y	
72.2	The role of Performer	Y	
73	Object of activity	Y	
74	Activity Date	Y	
75	Surplus from operating activities	N	
Relationships			
76	Link Identifier	Y	
77	Link between the initial object identifier	Y	
78	Link with the final object identifier	Y	

	Item Name	Mandatory	Condition
79	Link Type	Y	
80	Description Link	N	
81	Starting date The starting link	N	
82	Final date for the link	N	

I.2.1.6 Technical view

ABB- e-signing/Validation component



SBB: Digidoc

Electronic Signing of Documents is achieved using the DigiDoc System [51]. DigiDoc is a system that's widely-used in Estonia for storing, sharing and electronically signing documents. It is used by government institutions, businesses and private persons. It is also used to transmit files to other users in order to add digital certifications. In order to use DigiDoc you have to authenticate with an ID card or Mobile ID. Then a user can upload any document, digitally sign it, and forward it to other parties for their signatures.

Regarding the type of files that are supported, any type of e-Document can be entered for signature e.g. a word processing document, a photo, a plain text (e.g. messaging chat) or even voice recordings.

Regarding the persistency, the documents are stored in a unique folder for each user. Every time users log on, they see their own uploaded files and as well as any they have signed.

Regarding DigiDoc's adoption, the system is heavily used in Estonia's public sector, handling everything from court documents to municipal contracts. It's also commonly used in the banking industry, though its popularity in all areas of business is growing rapidly.

Regarding the Certificate format that is acceptable by DigiDoc, it is described in the Digital Signature Act [24]. According to this Act the Certificate format must contain:

- the number of the certificate;
- the name of the holder of the certificate;
- the public key of the certificate holder;

- the period of validity of the certificate;
- the issuer and registry code of the issuer; and
- a description of the limitations on the scope of use of the certificate.

Moreover, the Act contains clarifications regarding the following:

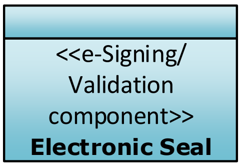
- Creation of private and public keys
- Application for certificates
- Period of Validity, and Suspension and Revocation of Certificates
- Certification Services and Certification Service Providers
- Time-stamping Services and Time-stamping Service Providers
- Termination of provision of certification services and time-stamping services
- State register of certificates
- Proprietary Liability of Service Providers and Insurance
- Supervision of Certification Service Providers and Time-stamping Service Providers
- Implementing Provisions

A more granular view of DigiDoc components is the following:

Client program: The DigiDoc Client program is available for everyone free of charge. It allows giving and checking electronic signatures. The DigiDoc Client program allows classification of data and converting classified data into a format that can be read by everyone.

Portal: The portal at the address digidoc.sk.ee is free of charge for all ID-card and Mobiil-ID holders and it allows giving and checking electronic signatures. Documents of any type can be signed in the portal and they can be sent to other users of the portal for signing, thereby creating multilaterally signed documents. There is also a 'lighter' version of the portal – the verification portal at the address https://digidoccheck.sk.ee. This allows checking the validity of electronic signatures, opening the initial files inside a DigiDoc file and preparing an electronic signature verification page for printing without an ID-card or logging into any service.

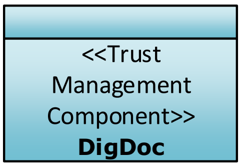
Web service: The web service serves the purpose of integrating DigiDoc with web-based information systems. The web service is used for easily integrating the functionalities of personal identification, signing and routing DigiDoc files with an ID-card and Mobiil-ID into an existing system. Client libraries and sample applications that simplify using the service have been created for various platforms in order to simplify using the web service.



SBB: Electronic Seal

Unlike electronic signatures given with an ID card, electronic seals are digital confirmations provided by legal persons. Sertifitseerimiskeskus (the Certification Centre) will issue one or several certificates for the use of an electronic seal. Different certificates can be used for different purposes [3]. Digitally stamped records can be opened with the DigiDoc software. Just as in the case of electronic signatures, the data on issuing and verifying the electronic seal are recorded in the DigiDoc container. If records are sent out with an electronic seal, the addressee can check whether the records have been sent by the right organisation or ascertain whether the person who sealed the records was authorised to act as a signatory on behalf of the organisation. This allows the addressee to be certain that the records sent to them have not been amended.

ABB- Trust Management Component



SBB:DigiDoc

DigiDoc supports the validation of certificates issued (and thus signatures created by them) by trusted Certification Service Providers under the supervision of the Ministry of Industry. As already analyzed in the organisational layer, multiple Certificate Service Providers are able to operate as-if they comply with the Digital Signature Act (DSA). CSPs may only be legal entities with a regulated minimum share capital and they must be entered in the National Certificate Service Provider Registry.

The National Registry of Certification Service Providers contains data about all Estonian CSPs and TSPs. Although it confirms the public keys of CSPs, it is technically not a root CA in Estonia. Instead, it functions as a supervisory authority, confirming the results of service providers' annual audits among other things. The Ministry of Economy and Communications, in whose administration area the registry works, has the right to verify audit results and inspect the service providers' premises and relevant information.

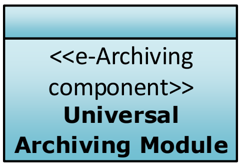
Encryption-Decryption

Encryption using the Estonian ID card, residence permit card or digital identity card is primarily intended to enable users to securely transfer records and single files containing sensitive information over an unsecured data communication channel (e.g. by e-mail). When encrypting the files, the user specifies the persons who have the right to decrypt them. This can be accomplished with the help of the card holders' public certificate directory (using an LDAP directory service). Since the encrypted files can only be opened by certificate holders who have been listed as addressees, the encrypting user must not forget to add themselves to the list of addressees if they might have to open the file later.

The DigiDoc Crypto application software is used for encrypting and decrypting with an ID card, a residence permit card or a digital identity card; the Mobile ID does not support encryption and decryption. The certificates for the Digi-ID chip and ID card are different, meaning that when the Digi-ID is used for encrypting data, the data cannot be decrypted with an ID card and vice versa.

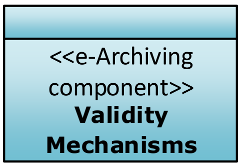
In order to decrypt data, the user needs a secret key that corresponds to the public key included in the authentication certificate and is ONLY available on the user's ID card or other digital identity document. The secret keys connected with the certificates of digital identity documents cannot be moved outside of the chip of the card and therefore no backup copies of the keys can be made. If an identity document becomes unusable or the certificate transferred to the document becomes invalid (e.g. when the period of validity expires or a new card is issued), the user can no longer open the records or files encrypted with the card earlier and no other individual than those listed as addressees can open them. All of the aforementioned circumstances have to be taken into account with regard to capturing and managing encrypted records in an ERMS; it is not recommended to store records in encrypted form if they have to be retained over a long period. Archives also refuse to accept encrypted records.

ABB- e Archiving Component



SBB: Universal Archiving Module

In order to facilitate the transfer of digital records with archival value to the archives, the National Archives have created a software tool: the Universal Archiving Module (UAM). UAM enables an archival scheme to be created using the classification scheme of an ERMS or its structure to be modified (as an example to merge classes). The records are exported from the ERMS to the UAM where they are (1) arranged and (2) described in accordance with the archival description rules. In the course of the arrangement, UAM enables the migration of records into file formats suitable for long term preservation (if necessary), etc. During the archival description phase, the archival description of the material is semi-automatically created based on the existing records management metadata.



SBB: Validity Mechanisms

Qualified signature specified in last section is secure enough provided that cryptographic algorithms used are unbreakable, key lengths are sufficient and private keys of CSP (the CA and OCSP key) remain under control of the service provider. Fast advances in computing suggest that key lengths and algorithms used today may not be secure enough in the future. There is also always a (theoretical) possibility that private key of some PKI service can get corrupted.

Additional measures are needed to protect electronic signatures from threats like those. Two mechanisms for maintaining long-time validity of electronic signatures are the following:

- **Logging**: service providing external evidence of certificate validity at the time of signing creates and maintains log containing issued responses
- **Archive time-stamp**: the whole material of the signature is periodically re-time- stamped

The first option does not require any end-user activity or additional functionality from BDOC-compliant system and therefore is preferred method. From the other hand the logging puts additional requirements to the service provider which may not be followed. In order to fully secure end-user and give him some additional independence of service provider, the archive time-stamp mechanism is also supported.

ABB- Data Routing Service

<<Data Routing Service>>
X-Roads

SBB: X-Roads

The functionality of Data Routing is delegated to the X-Roads layer as already discussed in the introduction. It is meaningful to clarify the following concepts that can be ambiguous:

- X-Road system [52]: it refers to the **data exchange platform** per se which covers the functionalities of routing and query-handling
- X-Road Protocol [53]: it refers to the data/e-Document adaptation procedures that are required in order for a structured-source to be "advertised" in the X-Road ecosystem (see Figure 20)

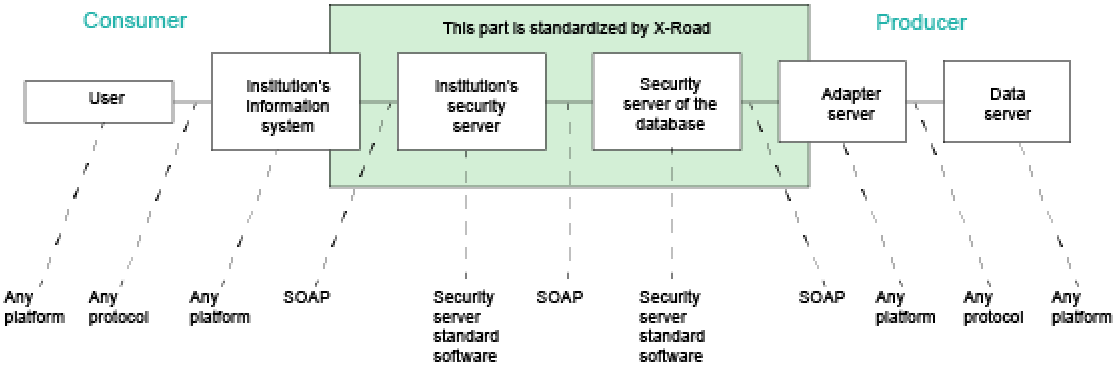

Consumer
This part is standardized by X-Road
Producer
User
Institution's information system
Institution's security server
Security server of the database
Adapter server
Data server
Any platform
Any protocol
Any platform
SOAP
Security server standard software
SOAP
Security server standard software
SOAP
Any platform
Any protocol
Any platform

Figure 20: X-Road Protocol

The X-ROAD system and protocol introduces some business-roles such as Service Provider, Service Consumer and Application Service Provider. In order to join the ecosystem some strict requirements have to be met [54]. From the technical perspective a fully documented API is provided in order to achieve X-ROAD on-boarding.

Additionally, a strict certification procedure is followed to re-assure successful on-boarding.

Finally, a “fork-project” of X-ROAD addressed as “X-ROAD EU” provides a simple infrastructure for cross-border services in domains not covered by existing EU and regional initiatives. X-Road EU uses a web service environment that is being developed for the public sector information systems of EU countries. It enables different information systems to exchange data safely and according to standards within the public Internet network. Safe architecture along with regulatory, organizational and technical measures are guaranteed in the X-Road EU web service environment.

In the X-Road EU environment, encrypted data are directly transferred through secure servers from one information system to another. Data can also be transferred to one system from multiple systems simultaneously. Data does not pass through the X-Road EU centre and cannot be viewed there. This guarantees the availability of data being exchanged on X-Road EU to the relevant parties solely. The centre only has statistical information about data transfer. Secure servers log the data traffic between themselves and send a hash to the central server.

The X-Road EU central server issues certificates to secure servers and provides a list of trusted certificates to systems connected to the X-Road. Additionally, the central server accepts log hashes from secure servers so that if needed, a chain of service usage can be constructed later. In this case, the service provider’s log, the service user’s log and the central server’s hash are compared. This method allows for checking the integrity of secure servers’ logs, as it is impossible to change a log without it being detectable later. Service users’ groups are described in the central server, so that service providers could open services to groups as well.

Finally, regarding the adoption of X-ROAD the following numbers are indicative:

- Over 170 databases offer their services over X-Road in Estonia.
- Over 2,000 services are used over X-Road in Estonia.
- Over 900 organisations use X-Road daily in Estonia.
- More than 50% of the inhabitants of Estonia use X-Road through the information portal eesti.ee.

I.3 Denmark

This annex provides an overview of e-Document solutions in Denmark.

I.3.1 Introduction

The Danish e-Government strategy 2011-2015 [55] is divided into three main tracks:

- The elimination of printed forms and letters;
- The establishment of new digital welfare;
- The adoption of digital solutions for closer public sector collaboration.

Towards these lines the Danish Government has established a group, in October 2002, in order to define a set of metadata for Electronic Document Management Systems in connection with the transmission of documents and cases from an Electronic Documents and Records Management System (hereinafter EDRMS) system to another. This working group has created the 'Standards for electronic file and document handling' (FESD-I) [56] specification which was amended on 2008 by the FESD-II specification [57].

In the frames of the latter specification all kinds of systems that are capable of handling case files and documents and operate under a Service Oriented Architecture (SOA), are taken under consideration. The new standards only define system service interfaces. The purpose of the standards is to facilitate interoperability and integration between all kinds of systems - including ERMS – which are handling case files and documents.

This will enable automation of the internal workflow in an organisation and ease exchange of case files and documents between different organisations. At the same time cost of integrations between systems can be reduced.

The standards are intended to be implemented by all public institutions with systems for managing case files and documents. These implementations are supposed to be conducted by system vendors, who therefore also are a target group for the standards. The overall target groups of the standards are then represented by both business and IT-technical expertise, which is reflected in the standards. The standards were drafted by workgroups, comprised of private vendors and representatives from public institutions. In 2009 specific standards were approved [58]:

- Standards for data exchange between public authorities (OIOXML)
- Standards for electronic file and document handling (FESD)
- Standards for electronic procurement in the public sector (OIOUBL)
- Standards for electronic signatures (OCES)
- Standards for public websites / homepages and accessibility
- Standards for IT security (DS484 - only for the government sector)
- Standards for document exchange (ODF/OOXML)

These standards are logically grouped in a reference architecture for records and case management which will be the focal point of our research. Furthermore, many private companies have released products that comply with the set of FESD-II specifications. One of this solutions, which is extensively used in Danish Administrations, is a software developed by developed by CBRAIN [59] named F2. Therefore, we will also include F2 in our analysis.

I.3.2 Reference Architecture for Records and Case Management

The Electronic Document and Record Management System (hereinafter EDRMS) reference architecture provides a framework for future standardisation in the field of document and records management. The EDRMS reference architecture must be used as a tool to prioritise what needs to be standardised and in which order. The target group for EDRMS reference architecture is public authorities and suppliers of IT solutions for the standardisation of records and case management. In addition, the Reference Architecture is relevant for organizations and private companies that have interfaces to government in the form of case and document- exchange, for example in connection with the reports, hearings, registration, file transfer, etc.

F2 Solution by cBrain

The cBrain F2 solution is a production platform for government work, developed in close collaboration with a number of Danish Ministries. It enables organisations to genuinely shift to a paperless model. Today 10 Danish Ministries use F2, including organisations with high security requirements such as the Prime Minister's Office and the Ministry for Foreign Affairs and municipalities such as "**Rudersdal Municipality**". The Ministry for Foreign Affairs is deploying F2 to over 100 locations globally.

The F2 Digital public administration suite is a fully integrated production platform that supports governmental working routines and knowledge production, informal and formal work, collaboration and communication. The F2 solution has the following functionality:

- Digital archive with advanced search;
- Role and access management;
- Records management/regulatory compliance;
- Management reporting and business intelligence;
- Chat;
- eGov workflow and processing;
- Collaboration;
- Communication including Email;
- Routing with input/output management;
- Case and document processing;
- Open interfaces (RESTful APIs);
- Open Document Standards (ODF, PDF/A);
- Single sign on via Active Directory; and
- Mobile access via smart phones & tablets.

In the frame of our analysis, F2 is a reference implementation of the aforementioned reference architecture. However, since our analysis was based on publicly disclosed technical and marketing material of the product, the goal was not to evaluate the F2-conformance to the reference architecture; but to extract information that could be mapped to the legal, organizational, semantic and technical layers below.

I.3.2.1 Legal view

The figure below presents an overview of the EIRA legal view in Denmark.

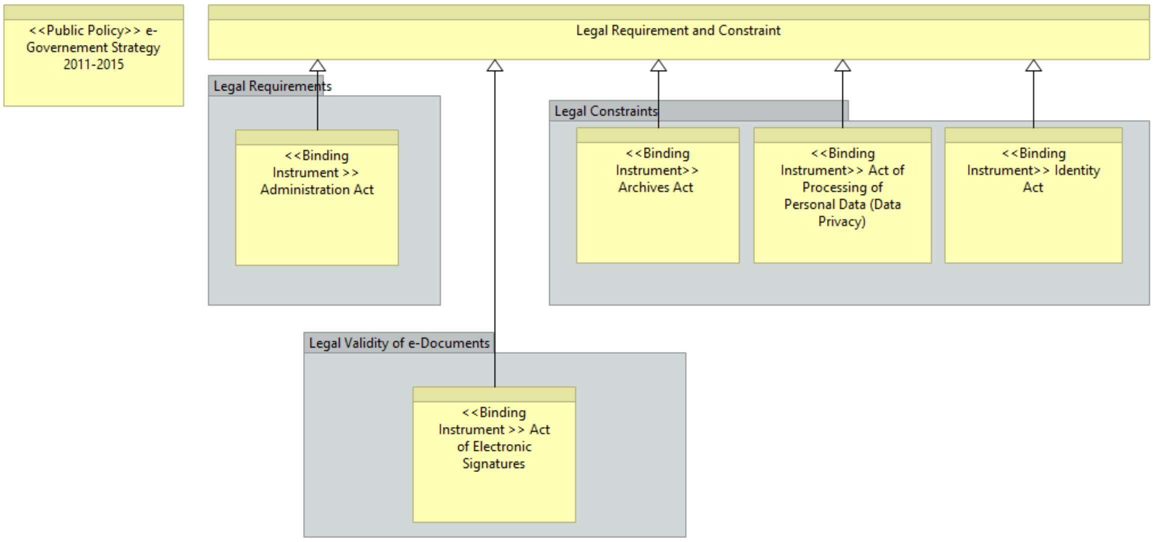

<<Public Policy>> e-Governement Strategy 2011-2015
Legal Requirement and Constraint
Legal Requirements
<<Binding Instrument >> Administration Act
Legal Constraints
<<Binding Instrument>> Archives Act
<<Binding Instrument>> Act of Processing of Personal Data (Data Privacy)
<<Binding Instrument>> Identity Act
Legal Validity of e-Documents
<<Binding Instrument >> Act of Electronic Signatures

Figure 21 Legal view in Denmark

ABB- Public Policy

SBB- E-government Strategy 2011-2015

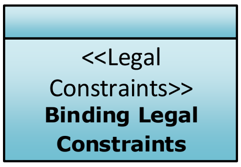
- **E-government Strategy 2011-2015** [55]**:** public authorities are required to use all relevant public sector solutions, to avoid developing parallel systems and to promote reuse of pertinent data. This will help to ensure that citizens experience a collaborative public sector. A section on internal digitization foresees the focus on digital document and archival handling systems.

ABB- Legal Requirements

SBB- Administration Act

- **Administration Act** [60]: The Act contains a number of general procedural rules including rules on rights of citizens regarding administrative procedures in various cases (time processing limits such as 10 days to respond to a citizen request etc.)

ABB- Legal Constraints



SBB- Binding Legal Constraints

The e-Document related processes (creation, archiving, routing etc.) have to meet specific constraints that are regulated by the law. Indicative constraints include the type of e-Document that should be preserved, the preservation period etc. The acts that impose most of these constraints are presented below:

- **Archives Act** [61]**:** The act covers the overall framework for preservation and disposal of records. According to the Act the public archives consist of the State Archives and local and regional archives. The State Archives consist of the National Archives and associated institutions. The State Archives are managed by the National Archivist. The National Archivist is appointed by the Minister for Culture. The objectives of the State Archives are:

  1) To ensure the preservation of records of historical value or which serve as documentation of matters of essential administrative or legal importance to the citizens and authorities;

  2) To ensure the possibility of disposal of public records of no preservation value in collaboration with the authorities covered by this Act;

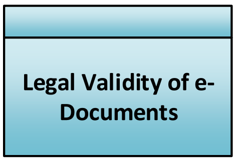
  3) To make records available to citizens and authorities, for example for research purposes;
  4) To guide citizens and authorities on how to use records;

  5) To carry out research and disseminate the knowledge of research results.

Is it a prerequisite for using an electronic platform for work in Denmark, that before going live the chosen electronic platform must have been technically approved by the national State Archives/the national archivist in order to document and ensure that relevant data in practice can be exported in the correct format for long term preservation at the National Archives. As an example, The F2 solution does therefore include functionality which support automated selection of relevant data (which could e.g. exclude informal discussions) and formatting for export including generation of special indexing and data summaries required by the standards defined by the National Archives.

- **Act of Processing of Personal Data (Data Privacy)** [62]**:** This Act shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

- **Identity Act**: Danish citizens are not required by law to carry an identity card. A traditional identity document (without photo), the personal identification number certificate (Danish:Personnummerbevis) is not much used in Danish society, as it has been largely replaced by the much more versatile National Health Insurance Card (Danish:Sundhedskortet) which contains the same information and more. The National Health Insurance Card is issued to all citizens age 12 and above however it does not contain embedded certificates that can be used for signing or authentication.

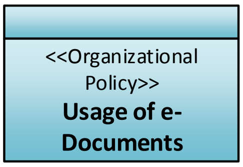


Specialization: Legal Validity of e-Documents

The legal validity of e-Documents relies on **the Act of Electronic Signatures** [63]: The purpose of the Act is to promote secure and efficient utilization of electronic communication by specifying requirements for certain electronic signatures and certification authorities that issue certificates for electronic signatures. The Act shall apply to certification authorities established in Denmark that issue qualified certificates to the public. The Act shall also apply to verification that signature-creation devices comply with the specified requirements for secure signature-creation devices.

I.3.2.2 Organisational view

ABB- Organisational Policy

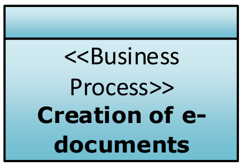


SBB- Usage of e-Documents in administrative processes

The various reference implementations of the architecture for records and case management facilitate the execution of administrative Government to Government processes. These processes may span from simple e-Document exchanges to complex case-handling. Indicative ministries and bodies that have adopted the F2 solution include:

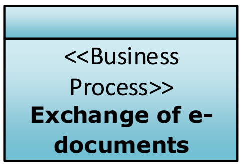
- Ministry of Social Affairs
- Ministry of the Environment
- Ministry of Climate and Energy
- Ministry of Economic Affairs and Interior
- Ministry of Transport
- Ministry of Employment
- Ministry of Gender Equality
- Ministry of Housing & Urban
- Ministry of Foreign Affairs
- Ministry of Finance
- Prime Minister's Office
- Agency for Digitisation
- Agency for Labour Market & Recruitment
- Danish Business Authority
- Danish Energy Agency
- Danish Meteorological Institute
- Gentofte Municipality
- The State Administration.

ABB- Business Processes



SBB: Creation of e-Documents

The creation of e-Documents is bound to the capabilities of the reference implementation of the platforms that comply with the "Documents and Case handling standard". Although in the standard there is no restriction for the generation process, there are indications of the file-types that are supported. As already discussed an e-Document may encapsulate all types of electronic files accompanied by their MIME type (doc, eml, mp4, etc.) along with descriptions that point to physical files. Therefore the generation process of the e-Document contents is practically unbounded. However the e-Document structure per se must be generated by a compliant software (e.g. F2 of CBRAIN).



SBB: Exchange of e-Documents

Regarding the exchange of e-Documents the Danish Agency of Digitization has generated a standard which progressively will be imposed to all IT systems of public authorities. This standard is OIOXML[20]. OIOXML refers to a common public language in the XML format providing the basis for creating coherence between the IT system of public authorities, as OIOXML ensures that information can be exchanged in a uniform and intelligible way.

OIOXML is a nationally developed XML dialect. Each data definition in OIOXML consists of two elements: a semantic definition and a syntax definition. All OIOXML specifications can be found on the digitaliser.dk portal where all specifications are provided. In future, public authorities need not establish special 'translators' for each individual purpose in order to exchange data with each other. When the entire public sector is using OIOXML, data can be exchanged and understood right away. Interoperability between IT solutions across the public sector is ensured by agreeing both on syntax and semantics for each individual concept in the exchange. Regarding OIO data definitions, semantics and syntax, OIOXML, like any other language, consists of a number of 'terms', each of which describes a concept, and which, taken together, can be combined to sentences or messages. A term describes a specific concept and is designated in OIOXML as an OIO data definition. An OIO data definition consists of two elements:

- An OIO semantic definition, describing the signification or meaning of the concept represented by the data definition.

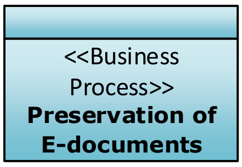
- An OIO syntax definition, describing the physical XML format used to represent the concept in a specific OIOXML message. The syntax definition is specified in an OIOXML schema, i.e. an XML schema complying with the XML Schema recommendation as well as the nationally developed set of rules, known as OIO Naming and Design Rules (NDR).

It is essential to a meaningful exchange of information that semantics and syntax are closely linked together in a data definition. As a consequence, a syntax definition (an OIOXML schema) cannot stand alone. It must exist together with a semantic definition in order to form a data definition.

SBB: Access to e-Documents

The responsibility to access and control e-Documents is delegated to the implementations of the reference architecture. In case of F2, it is possible to define multiple user role types with individual functional rights as far as e-Documents handling is concerned. Furthermore, it is possible to define full organisation chart and assign roles and users (for specific e-Document actions). The users can be imported from the public-body’s active directory.

[20] http://www.digst.dk/Servicemenu/English/IT-Architecture-and-Standards/Standardisation/Standardisation-creating-digital-Denmark/About-OIOXML



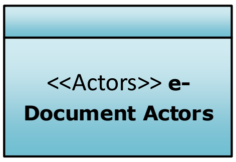
SBB: Preservation of e-Documents

According to the Danish Archiving Act each public body that handle e-Documents has to maintain archives. As already discussed, the public archives consist of the State Archives and the local and regional archives. In a nutshell, the objectives of the State Archives are a) to ensure the preservation of records of historical value b) to ensure the possibility of disposal of public records of no preservation value c)to make records available to citizens and authorities d) to guide citizens and authorities on how to use records and e) to carry out research and disseminate the knowledge of research results.

The authorities shall ensure the safety and integrity of archives, including that records are kept in a satisfactory manner. The authorities shall ensure that records stored on electronic media be kept in such a manner that they can be transferred to public archives. When records are transferred to public archives the responsibility for their future preservation shall pass to the said public archives.

Any software version that complies with the Reference Architecture is obliged to comply with an archiving schema that is imposed by the National Archives. This schema is used during the indexing of the e-documents. Finally, the accessibility to the archived material is regulated by the Archiving Act and is dependent to the nature of the information. Indicatively, archival units created or provided by the public administration and the courts of law and which have been transferred to public archives, are accessible when the archival units are 20 years old.

ABB-Actors



SBB: e-Document Actors

The main actors that play an active role in e-Document processes are civil servants that generate and handle e-Documents and Process managers that map the organisational diagrams and the business processes to a systemic view. This configuration is essential since some workflows do not adhere to a process model (e.g. exchange of emails) yet some workflows adhere to strict case-handling. This differentiation should be tackled by any implementation of the reference architecture.

I.3.2.3 Semantic view

ABB-Data Model

<<Data Model>> **e-Document**

SBB: e-Document

The structure of e-Document is defined by a dedicated committee (OIO committee) and is provided here [64]. All Case and Document handling systems should comply with the specific meta-model which is presented in the figure below. More specifically, an e-Document consists of the actual document-part, such as a spreadsheet or Annual Report and the metadata that describe the document. Indicative metadata include document title, document date etc. In most cases, the actual documents consist only of electronic files, whether they are produced electronically or they are converted into electronic form (through scanning). But in some cases, the actual documents may be in a natural variant either supplemented with an electronic reference or completely free of electronic link. The prevalence of physical variants typically applies at large documents that are difficult to scan, including thick manuals or technical drawings.

Electronic documents may be available in many different formats, including word processing documents, presentations, spreadsheets, databases, scanned documents, PDF, HTML, TIFF, audio files, image files and video files. Electronic documents consist of one or more variants; each consisting of one or more parts.

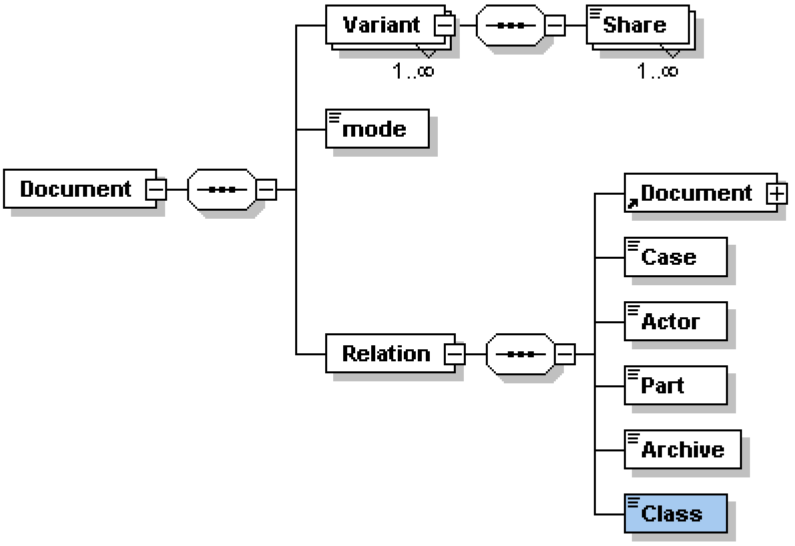


Figure 22 - e-Document format according to OIO Standards

The concept of Variant is used to manage the same logical document in various situations. For example, the same document can be found in an e-mail format, in a JPEG and in a TIFF format. The first format is used for case processing of incoming email, while the other is used during archiving. Document Variants are thus used for different but complementary purposes. Variant formats are also described in a respective Variant-schema.

Furthermore, an e-Document may consist of document parts. Document parts are used to handle different but complementary parts of documents. For example, three document parts may contain three different chapters of a report. This breakdown of a document to elements may be appropriate when several actors (editors) are working on the same document simultaneously. Document parts may also contain other document parts. For example, an e-mail with two attachments (a picture and a spreadsheet) is considered a compound document with two document parts that can be handled independently.

Different document versions in the same document object have rarely the same number of document parts. Typically there is one production variant with multiple document shares, multiple publication variants with one composed Document element and one or more archival versions each with a document part. Document parts can be reserved and released independently of each other.

This mechanism ensures that document-editors are not working on the same document at the same time. Document parts that are reserved by a given actor can only be released by the same actor. Document parts that are released, however, can be updated by all stakeholders with appropriate rights. The specification does not dictate how the document composition process is achieved.

A common attributed of document variants and document parts is that they all share the same document version. This means that changes in documents' metadata (attributes, conditions and relationships) and content (the binary file) are recorded and can be reviewed over time. This practically replaces the classic version control system where each new version is bound to a new copy of the entire set of metadata and content. However, version numbers and update-dates should accompany the version metadata.

Moreover, each e-Document may be related to other elements e.g. e-Documents. The following table summarizes these relationships:

Description	**Object Type**	**Cardinality**
Archives, which document belongs	Archive	1..n
Documents that reply to this document	Document	0..n
Documents that are the basis for this document	Document	0..n
Document, that is a new revision of this document	Document	0..1

Documents that comments on this document	Document	0..n
Documents attached to this document	Document	0..n
Documents which this document relates to. Relation purpose noted in the relationship.	Document	0..n
Class in a classification system that classifies this document. This is the primary classification of the document.	Class	0..1
Actor which owns the document	Stakeholder	1..1
Operator who is responsible for the document	Stakeholder	1..1
Actors, working with/treats documents.	Stakeholder	0..n
Actor, as the document is distributed to	Stakeholder	0..1
Parties who have submitted the document to the authorities authority or has received the document from authority	Stakeholder	0..n
The parties which have received authorized copy of the document	Stakeholder	0..n
Cases in which the document is attached	Stakeholder	0..n

A formal XSD schema for the e-Document document definition is provided here [65]. On overview of the e-Document complex-type is provided below:

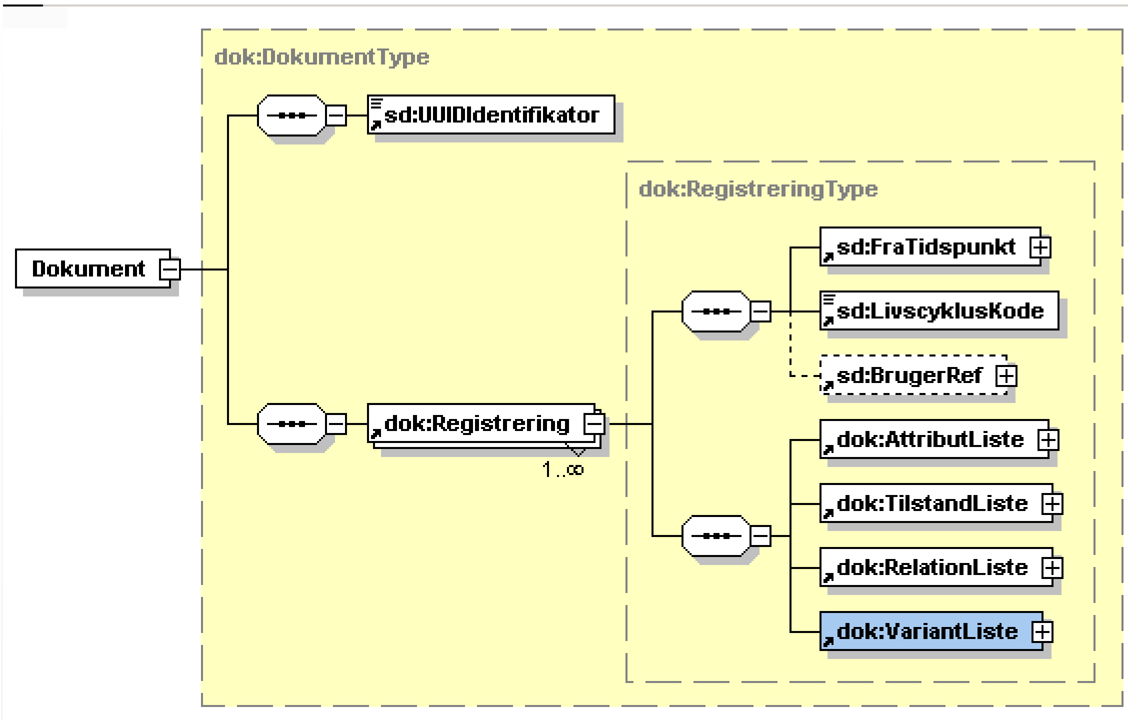


Figure 23 - e-Document XSD complex-type

<<Data Model>> **e-File**

SBB: e-File

The term e-File can be used to describe the notion of a compound document. According to the e-Document schema (see e-Document definition above) each document may be associated with other documents or with other document-parts. This grouping is practically a logical e-File which can be used during a case-handling workflow. What is of major importance is that in case of Denmark each e-Document can be potentially extended to an e-File.

ABB- Metadata

<<Metadata>> **Metadata**

SBB: Metadata

Work on the Danish Reference Architecture is inspired by the following international standards:

- NOARK5 is the Norwegian standard for requirements for electronic case and records in public
- MoReq2 is an EU standard for "records management" system based on ISO 15489
- ISO 15489 Information and documentation - International standard for archive
- ISO 23081 Information and documentation - Records management processes & Meta data records. This is an international metadata standard for archival documents
- ISO 14721 Reference Model for an Open Archival Information System (OAIS). This is a reference architecture for archiving.

As an extension to the Fesd-1 standard, the Fesd-2 standard takes a broader view on the e-document and the whole document lifecycle. This has strongly influenced the F2 solution implementation and as a consequence, the metadata model has now been divided into a set of logical components with a comprehensive set of metadata in order to support informal/formal work in parallel with control and organization elements as well as communication and workflow/processes. The metadata model is presented on Figure 24

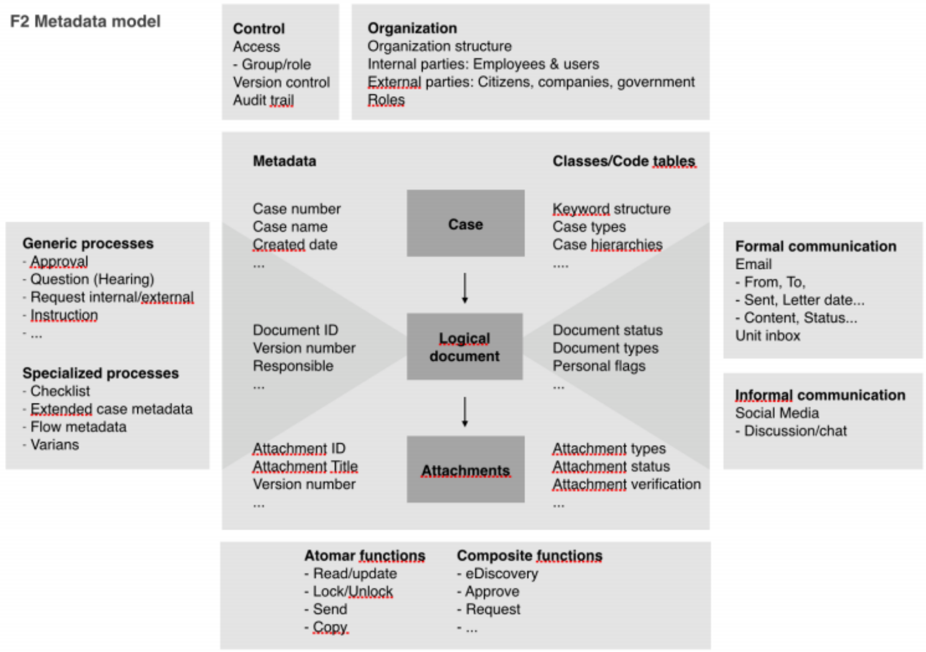


Figure 24 - cBrainF2 Metadata Model

Table 5 – Metadata Model Description

Metadata Component	Description
E-document	The fundamental organisation of e-documents are based on 3 layers:

Metadata Component	Description
	- Case (which is optional) organising records into logical groups (like folders), which is the base for work processing - Logical document, which can be described as a MoReq2 container - Attachments, which hold contents in different formats like Word, Excel etc. The Danish 3-layer model is similar to the German Domea Neu model, which refers to the 3 layers as: - Vorgang - Dokumente - Schriftstück At all 3 levels, metadata as well as classes/codes are attached
Control	Metadata to ensure Legal, access, audit trails and versioning
Organisation	Metadata that support definition and setup of organisation, based on roles. This includes internal organisation (like employees) as well external parties. Organisation is tight connected to Control thereby supporting e.g. validity and identification
Formal communication	Metadata to suppprt communication which is part of a formal proces (and which often requires signature). Formal communication includes electronic post.
Informal communication	Metadata to support discussions and informal exchanges. In F2 Informal Communication is supported by a Chat-like mechanism in the context of the record, and metadata for informal communication thereby relates to the record. Note: In the German Domea Neu standard

Metadata Component	Description
	informal communication is a core part of the E-zusammenarbeit ("Bausteine").
Generic processes	Metadata that support processes which are not tied to specific work areas. Examples of generic processes are approval process or request for work.
Specialised processes	Metadata that support work specific processes and workflows. In contrast to traditional BPM-based models (Business Process Management), there has as part of the Danish F2 model been developed a checklist-based model to support specific government work processes, as Danish experiences show that traditional BPMmodels often fail when it comes to support case processing in public administration.
Atomar functions	Metadata related to the core system functions like update record (not a database function, but a logical function). Atomar functions defines the set of core operations which users can operate as part of work processing. Atomar Functions functions are fundamental to offer open data and open system/ system-system integration. As an example in the F2 solution Atomar Functions are not only used within the F2 system itself, but also exposed as REST-API's.
Composite functions	Metadata related to high-level functions, covering a group of Atomar Functions. This allow for e.g. across government collaboration and data exchange like E-discovery.

I.3.2.4 Technical view

ABB- Identity Management Component

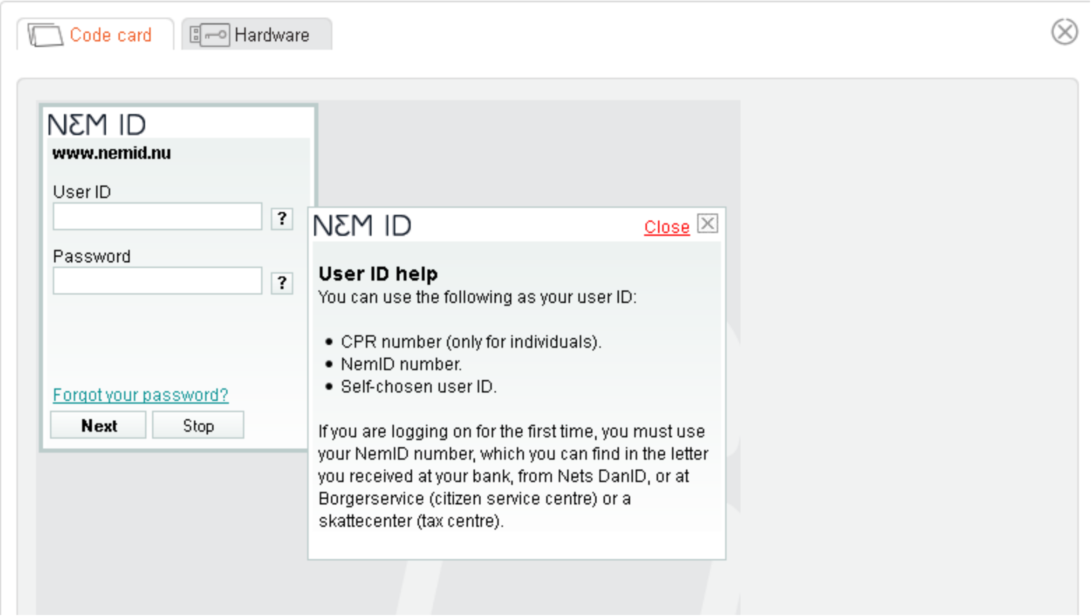
<<Identity Managment component>>
NEMID

SBB: NEMID

Authentication is achieved using the **nemid.eu** access portal. There are two possibilities

a) to use a set of credentials that are distributed to the citizen by a public service;

b) to use a Hardware Security Module (HSM) which contains one qualified certificate;



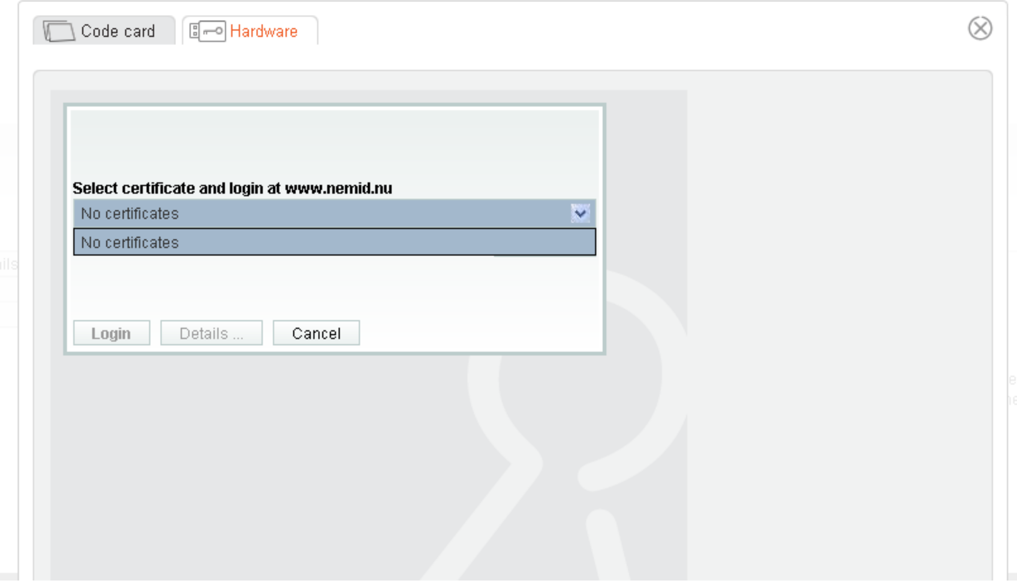
User ID help

You can use the following as your user ID:

- CPR number (only for individuals).
- NemID number.
- Self-chosen user ID.

If you are logging on for the first time, you must use your NemID number, which you can find in the letter you received at your bank, from Nets DanID, or at Borgerservice (citizen service centre) or a skattecenter (tax centre).

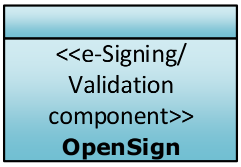
Figure 25: Pre-shared Key based Identity Management



Select certificate and login at www.nemid.nu

Figure 26: Certificate based Identity Management

ABB- e-Signing/Validation component



SBB: OpenSign

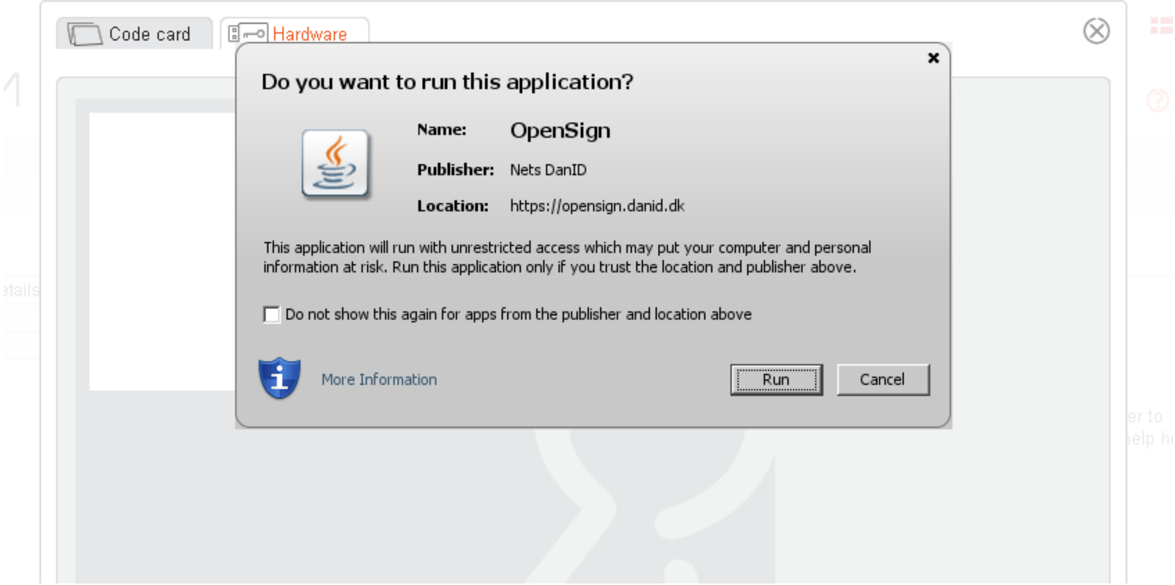
Danish electronic signature is primarily used in communication between private enterprises and public authorities in Denmark. Approximately 120.000 companies, and more than 325.000 employees in Denmark have an Electronic signature. The electronic signatures are partly free of charge for the private enterprises, but with a transaction-fee to DanID, from the merchants, who benefits from using the infrastructure.

There are some citizen-certificates (called "OCES1 Personal certificates") issued using DanID solution, but issuance has ended in 2010. Please note that the enterprises-part of the Danish electronic signature (called "OCES1 Medarbejdersignatur") was expected to be replaced by NemID during 2012/2013. Finally, **NemID** has prevailed for both authentication and Signing [66].

Electronic signature and Verification is achieved using the OpenSign component [49]. OpenSign provides the following features

- electronic signing of text
- support for x.509 certificates stored in PKCS12s
- support for x.509 certificates stored in the Microsoft Windows Keystore (CAPI)
- support for the native Microsoft Java virtual machine
- works in all common browsers: Firefox, Internet Explorer, Mozilla, Safari, etc.

- has a small footprint: The core applet is less than 100KB.
- has localization support



Do you want to run this application?

Name: OpenSign

Publisher: Nets DanID

Location: https://opensign.danid.dk

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

☐ Do not show this again for apps from the publisher and location above

Figure 27: OpenSign for Signing/Verification

According to NemID-Interoperability-Guide [67] Signing and Verification of Signatures are provided at the level of:

- TEXT plain, unformatted text
- HTML
- XML
- PDF

Time stamping service is also provided; yet no electronic sealing.