eID Solution Architecture Template (SAT)

v1.1.0 - Beta

Change control

Modification	Details
Version 1.0.0 Beta	

Disclaimer:

TABLE OF CONTENTS

1 INTRODUCTION

This document contains the description for a Solution Architecture Document (SAT) for eID cross border authenticated service.

This SAT is based on EIRA v1.1.0

The ArchiMate source are embedded in this document in the "Archi format" as well as in "The Open Group ArchiMate Model Exchange File Format".


SAT_eID_v1_0_0_Beta.archimate


SAT_eID_v1_0_0_Beta.xml

1.1 Purpose of this document

Enterprise and Solution architects can use this document to design solution architectures in the domain of eID cross border authenticated service.

1.2 List of acronyms used in this document

Table 1-1

ABB	Architecture Building Block
CEF	Connecting Europe Facility
DIGIT	Directorate-General for Informatics
EC	European Commission
eIDAS	Electronic Identification and Trust Services for Electronic Transactions in the Internal Market
EIRA	European Interoperability Reference Architecture
EU	European Union
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
INEA	Innovation and Networks Executive Agency
IP	Internet Protocol
SAML	Security Assertion Markup Language
SAT	Solution Architecture Template
SLA	Service Level Agreement
SBB	Solution Building Block
TLS	Transport Layer Security

2 GOAL, DESCRIPTION AND TARGET AUDIENCE

This chapter gives the goals and a description on eID cross border authenticated service and indicates the target audience and their potential use of this Solution Architecture Template (SAT).

2.1 Goal

The purpose of this SAT is to provide guidance by defining minimal, but holistic (legal, organisational, semantic and technical) interoperability architecture to implement a eID cross border authenticated service. The eID SAT should allow businesses and public administrations to have a common understanding of the most-salient building blocks from the perspective of interoperability.

2.2 What is eID

The CEF eID building block helps public administrations and private online service providers to easily extend the use of their online services to citizens from other EU Member States. It allows cross-border authentication, in a secure, reliable and trusted way, by making national electronic identification systems interoperable.

Once this building block is deployed in a Member State, the mutual recognition of national eIDs becomes possible between participating Member States, in line with the eIDAS (electronic Identification and Signature) legal framework (see eIDAS Regulation (EU) 910/2014[1]) and with the privacy requirements of all the participating countries. Mutual recognition of national eIDs allows citizens of one Member State to access online services provided by public and private organisations from other participating EU Member States, using their own national eID.

Following the successful completion of the STORK pilot programme, CEF has taken on the role to 'productise' and support the roll-out of eID connectivity to other Member States. This has included the development of open-source software components, documentation, training and support. Member States can leverage their electronic ID systems to provide access to the services of other Member States with confidence in the levels of assurance provided by secure means of authentication linked to qualified identities.

The technical management of the eID building block DSI is done by the Directorate-General for Informatics (DIGIT) of the European Commission.

Implementation of the EU policy directly related to eID and Trust Services is the responsibility of the Directorate-General for Communications Networks, Content and Technology (DG CNECT) of the European Commission.

The Innovation and Networks Executive Agency (INEA) is responsible for the implementation of the CEF Telecom programme grants in cooperation with the Commission.

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

2.3 What is a solution architecture template (SAT)

A Solution Architecture Template (SAT) is a specification extending the EIRA providing support to solution architects in a specific solution domain. An SAT contains a motivation (principles, requirements), a goal and a description of the supported functionalities, a sub-set of the EIRA core Architecture Building Blocks (ABBs) covering the four views, a set of specific ABBs extending EIRA's views enabling specific functionalities to be provided by implementations derived from the SAT and the interoperability specifications of selected ABBs and a narrative for each EIRA view.

The benefits of a SAT are the following:

- Provides architects with a common approach to cope with a specific interoperability challenge. It also places the focus on the key-points you need to consider.
- An architect can create a solution architecture by mapping existing Solution Building Blocks (SBBs) to an SAT, based on the interoperability specifications that are provided. This is done by providing SBBs for the ABBs identified in the SAT.
- When an architect creates an SAT, he/she can define the interoperability specifications for the SAT's ABBs and moreover recommend specific SBBs which produces faster and more interoperable results.
- An SAT can be created within and across the different views of the EIRA. An SAT can then support architects specialised in different interoperability levels."

2.4 Target audience

This document has the following target audience:

Table 2-1

Audience	Description
Architects	Enterprise/solution architects involved in the design and operation of eID cross border authenticated service.
Service providers	Service providers involved in the implementation and roll-out of eID cross border authenticated service.

3 eID INTEROPERABILITY MAPPED TO THE EIRA

This chapter contains for each EIRA view the corresponding ArchiMate model and narrative. Next to the SAT's EIRA architecture building blocks, the ArchiMate model includes, where applicable, the related specifications, principles and requirements.

The models have been scaled down to fit with the text, they are included in bigger format in the appendix.

3.1 How to use this SAT

An architect that uses this SAT typically wants to perform a gap-analysis between an existing solution and this Solution Architecture Template, or he/she wants to model a solution in the domain of eID cross border authenticated service and uses this document as guidance.

3.1.1 Gap Analysis

Using this SAT for gap analysis, the architect can map the building blocks of the solution to the ones in this SAT and identify which building blocks are missing. These building blocks can either indicate missing functionality or missing interoperability specifications.

3.1.2 Building a solution

When building a solution, the architect is expected to use the four different EIRA views and provide a solution in the form of Solution Building Blocks (SBBs) for the Architecture Building Blocks (SBBs) that are indicated. This is done by replacing the Architecture Building Block (ABB) with an annotated Solution Building Block. The existing Solution Building Blocks (SBB) in this SAT should not be removed and replaced, however, the acknowledgement of reusing these building blocks can be done by removing the ABBs which they specialise.

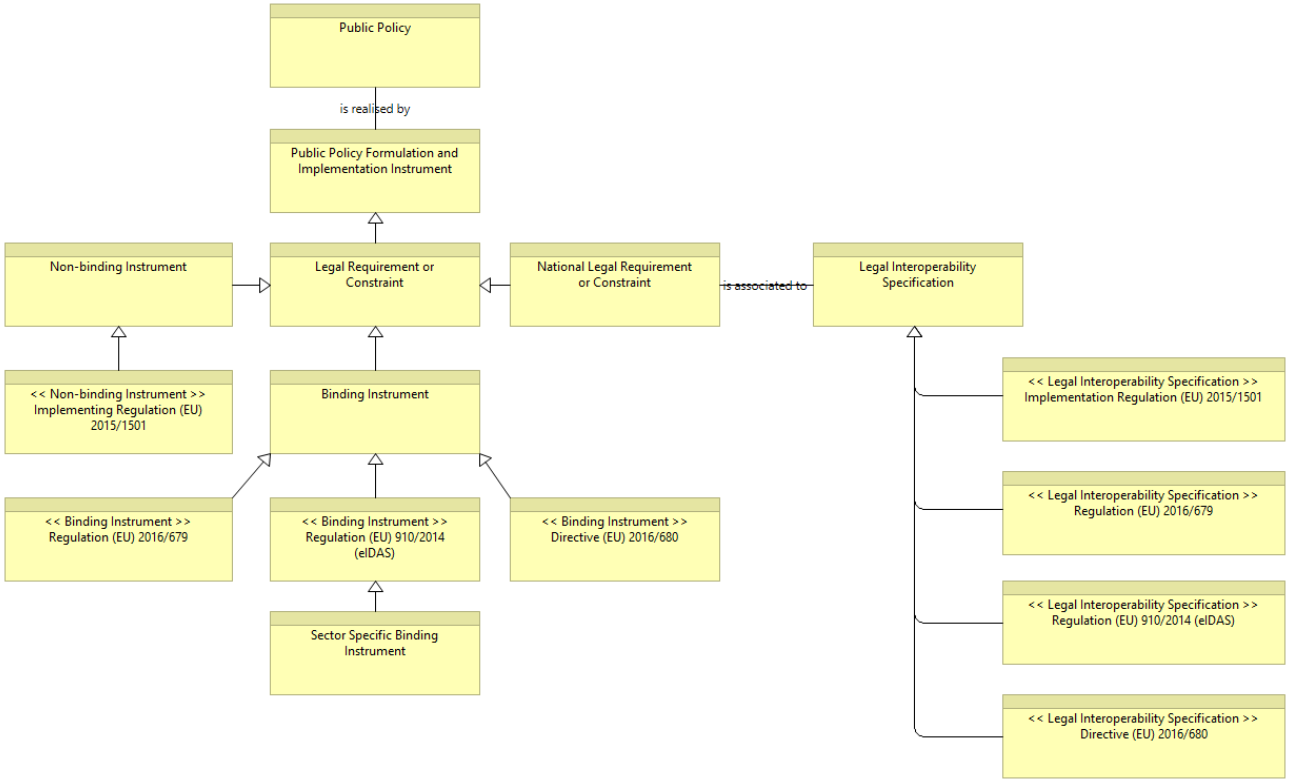
Interoperability Specifications (IoP specs) are added as specialisation of an Interoperability ABB, implemented in the form of an SBB and attached to an ABB as interoperability requirements. The final solution should only contain the implementation (the SBB) of the IoP Spec

The result will be a solution architecture that will contain only SBBs, all ABBs should have been removed (in the case this SAT already provides SBBs for this ABB) or replaced by SBBs (solutions that implement that ABB).

The SAT is a document describing the needed Architecture Building Blocks for a desired solution. This should not be taken as restrictive but as advisory. When an Architecture Building Block (ABB) is present for which there is no implementation foreseen in the form of a Solution Building Block (SBB), it is *strongly* recommended, but not mandatory, to take this ABB into consideration in the final solution.

3.2 Legal View

The Legal view of the eID SAT consists of the following sub-set of EIRA Architecture Building Blocks (ABBs) as well as some predefined Solution Building Blocks (SBBs):



The eIDAS Regulation provides a solution to ensure the cross-border mutual recognition of eID means.

The Commission published the technical specifications and reference implementations of the interoperability nodes for the eID mechanisms on 26 November 2015 for the technological infrastructure under Connecting European Facility program (CEF) as open source.

Since 29 September 2015, following the adoption of the implementing acts on cooperation between Member States on eID, on interoperability framework, on assurance levels for eID means and on notification, EU Member States may notify and recognise, on a voluntary basis, national eID means. As of 29 September 2018 the recognition of notified eID will become mandatory.

This means that EU citizens will be able to use the eID means they use at national level also to access public services across borders in other Member States.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Regulation sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data.

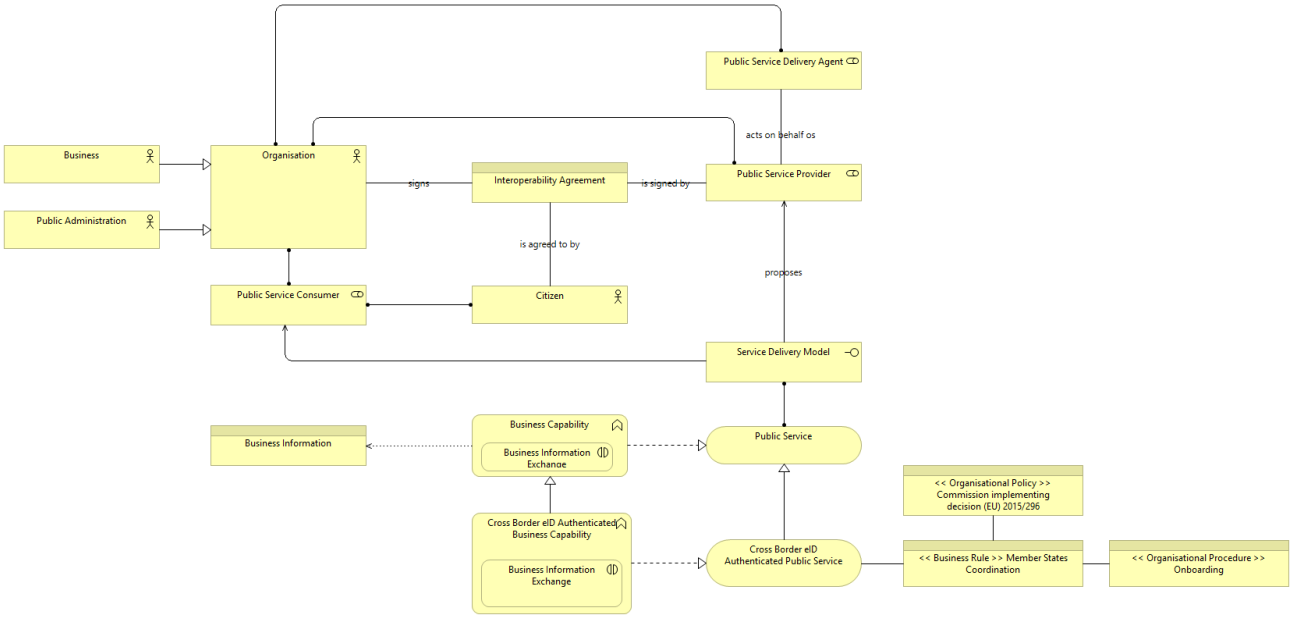
Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent

authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. It will in particular ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism.

On top of those instruments, depending on the sector of activity of the implementation, one should consider the addition of sector specific binding instruments.

3.3 Organisational View

The Organisational view of the eID SAT consists of the following sub-set of EIRA Architecture Building Blocks (ABBs) as well as some predefined Solution Building Blocks (SBBs):



This SAT is Business Capability agnostic, as long as the business capability requires a cross border eID authentication.

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

According to this decision, CEF eID, via its eIDAS Cooperation Network, undertakes the task of general coordination of the eID activities in the Member States, in order to:

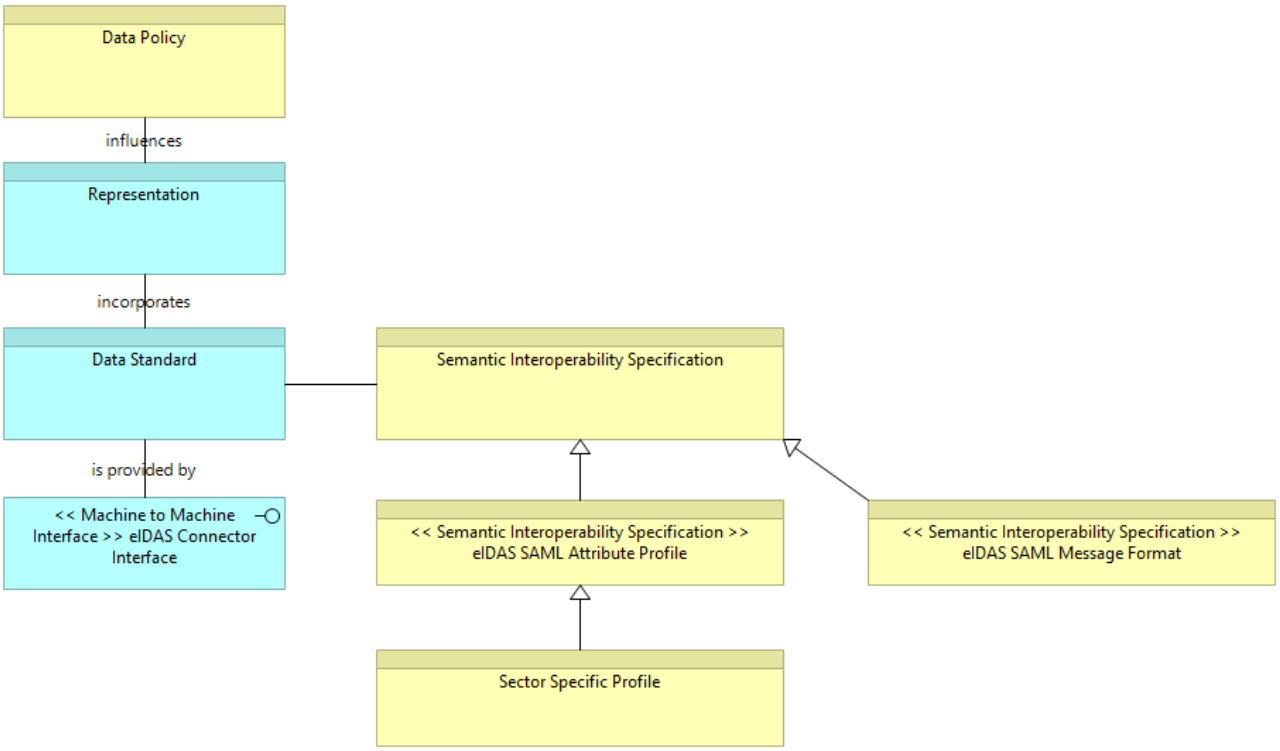
- Ensure maximal interoperability of the eID core service platform across borders
- Advise to support the eIDAS compliance in the Member States, from a legal to technical point of view.

In order to facilitate the on boarding, eIDAS Cooperation Network provides "Point of single contact" for each member states that can be found here:

https://ec.europa.eu/cefdigital/wiki/display/EIDCOOPNET/Points+of+single+contact

3.4 Semantic View

The Semantic view of the eID SAT consists of the following sub-set of EIRA Architecture Building Blocks (ABBs):



The technical specifications for the eIDAS interoperability framework have been developed by the European Commission with the help of member states collaborating in a technical sub-committee of the eIDAS Expert Group. A further role of the Commission has been to provide a sample implementation of the technical specifications which member states are free to adopt as an "off the shelf" implementation should they wish to do so.

The specifications posted here as versions 1.0 represent a stable eIDAS compliant set of technical specifications which Member States can use if they are providing their own implementation. These technical specifications will be subject to further development in the normal course of events and any subsequent changes will form part of the timed release management process.

The Version 1.0 technical specifications consist of four separate documents, each concerning a specific area.

On semantic level, two of the four specifications should be considered:

- eIDAS SAML Message Format[2]
- eIDAS SAML Attribute Profile[3]

The eIDAS interoperability framework including its national entities (eIDAS-Connector and eIDAS Service) need to exchange messages including personal and technical attributes to support cross border identification and authentication processes. For the exchange of messages, the use of the

[2] https://ec.europa.eu/cefdigital/wiki/download/attachments/23003348/eidas_message_format_v1.0.pdf?version=1&modificationDate=1457112918000&api=v2

[3] https://ec.europa.eu/cefdigital/wiki/download/attachments/23003348/eidas_saml_attribute_profile_v1.0_2.pdf?version=1&modificationDate=1457112919000&api=v2

SAML 2.0 specifications has been agreed in the eIDAS technical subgroup and is laid down in the eIDAS Interoperability Architecture.

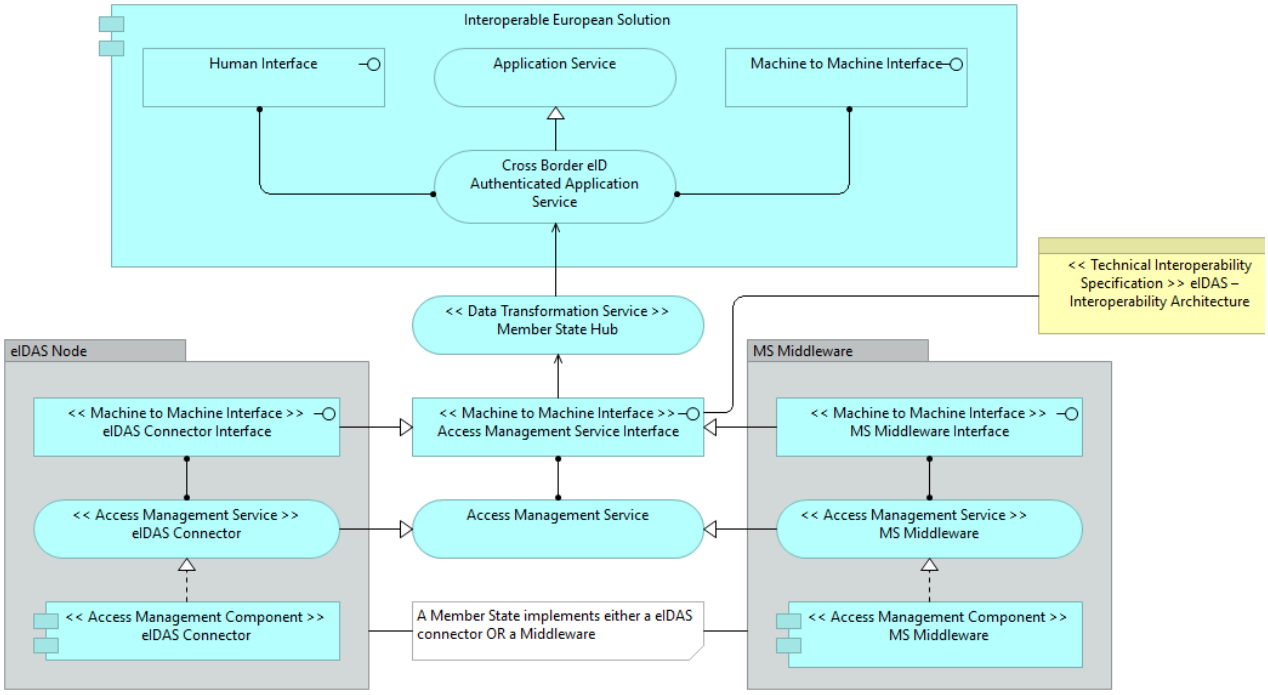
Since the eIDAS interoperability architecture should use widely used standards, the following SAMLbased profiles are taken into utmost account in this paper:

- Kantara Initiative eGovernment Implementation Profile of SAML V2.0 [SAMLeGov2.0]
- STORK 2.0 D4.4 First version of Technical Specifications for the cross border Interface [STORK]

eIDAS specifications are meant to be generic, depending on the sector of activity of the implementation, one should consider the addition of sector specific specifications, like additional SAML attributes.

3.5 Technical View – Application

The Technical application view of the eID SAT consists of the following sub-set of EIRA Architecture Building Blocks (ABBs) as well as certain non EIRA Architecture Building Blocks and predefined Solution Building Blocks (SBBs):



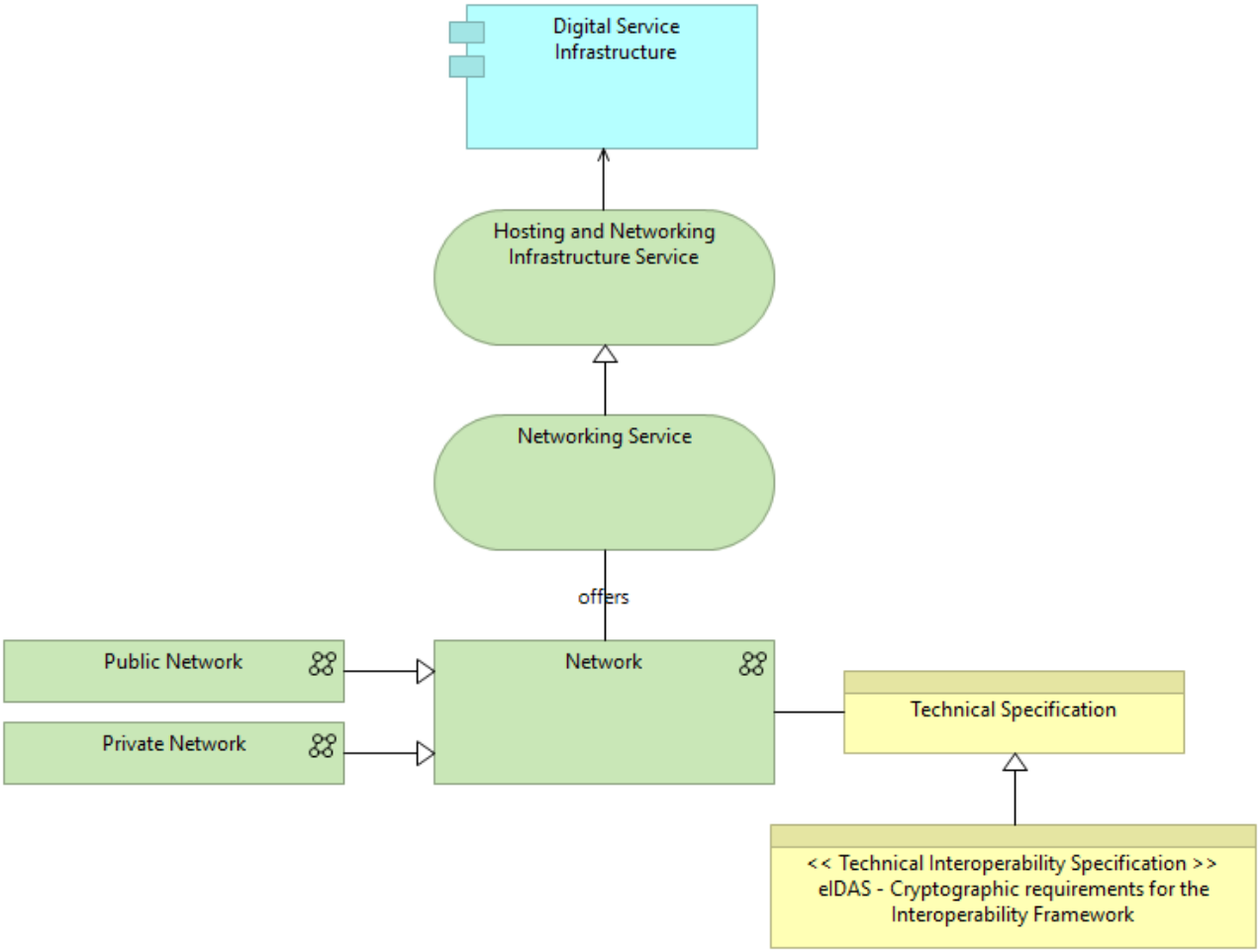
Cross border authentication via eID is achieved via the 'eIDAS-Network'. The 'eIDAS-Network' consists of eIDAS-Nodes, which can either request or provide a cross-border authentication. In the case of the request of a cross border authentication, this can be done two different ways:

- Via the eIDAS Node's connector: the authentication request will be addressed to the connector that will get the authentication information.
- Via Middleware-Service: the authentication request will be addressed to the member state middleware that will get the authentication information.

The technical specifications of the eIDAS connector or the MS Middleware follow the technical specifications for the eIDAS interoperability framework (eIDAS – Interoperability Architecture[4]) and are provided at national level.
Depending on the Member State, connection to the eIDAS Node can be done through a national hub. Information concerning this hub can be asked at national level.

3.6 Technical View – Infrastructure

The Technical infrastructure view of the eID SAT consists of the following sub-set of EIRA Architecture Building Blocks (ABBs) as well as some predefined Solution Building Blocks (SBBs):



Within the eIDAS Interoperability Framework, communication between eIDAS nodes (i.e. eIDAS-Services and eIDAS-Connectors) is performed via the citizen's browser. Here, the content of the communication between eIDAS nodes is performed using cryptographically protected SAML messages. To secure the transport layer of this communication between these components and the citizen's browser, TLS is used. The technical specifictions for eIDAS crypto requirements specifies cryptographic requirements for the protection of the SAML communication as well as on the usage of TLS within this communication.

[4] https://ec.europa.eu/cefdigital/wiki/download/attachments/23003348/eidas_interoperability_architecture_v1.00.pdf?version=1&modificationDate=1457112919000&api=v2

4 REFERENCES

- CEF digital eID

  https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID
- eSens eID SAT

  http://wiki.ds.unipi.gr/display/ESENS/WP6+-+Building+Blocks
- European Interoperability Reference Architecture (EIRA)

  https://joinup.ec.europa.eu/asset/eia/
- European Interoperability Framework (EIF)

  http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf
- ArchiMate®

  http://www.opengroup.org/subjectareas/enterprise/archimate
- Archi®

  http://www.archimatetool.com/

4.1 Legislative references

- Regulation (EU) N°910/2014 (eIDAS)

  http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
- Implementing Regulation (EU) 2015/1501

  http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0001
- Regulation (EU) 2016/679

  http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
- Directive (EU) 2016/680

  http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l14012&from=EN

4.2 Organisational references

- Commission implementing decision (EU) 2015/296

  http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D0296
- CEF Digital Member States Coordination

  https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Member+States+coordination
- eIDAS Cooperation Network

  https://ec.europa.eu/cefdigital/wiki/display/EIDCOOPNET/eIDAS+Cooperation+Network

4.3 Semantical references

- eID eIDAS Profile

  https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+eIDAS+profile
- eIDAS Message Format

https://ec.europa.eu/cefdigital/wiki/download/attachments/23003348/eidas_message_format_v1.0.pdf?version=1&modificationDate=1457112918000&api=v2

- eIDAS SAML Attribute Profile

  https://ec.europa.eu/cefdigital/wiki/download/attachments/23003348/eidas_saml_attribute_profile_v1.0_2.pdf?version=1&modificationDate=1457112919000&api=v2

4.4 Technical references

- eIDAS Interoperability Architecture

  https://ec.europa.eu/cefdigital/wiki/download/attachments/23003348/eidas_interoperability_architecture_v1.00.pdf?version=1&modificationDate=1457112919000&api=v2

- eIDAS crypto requirements for the eIDAS Interoperability Framework

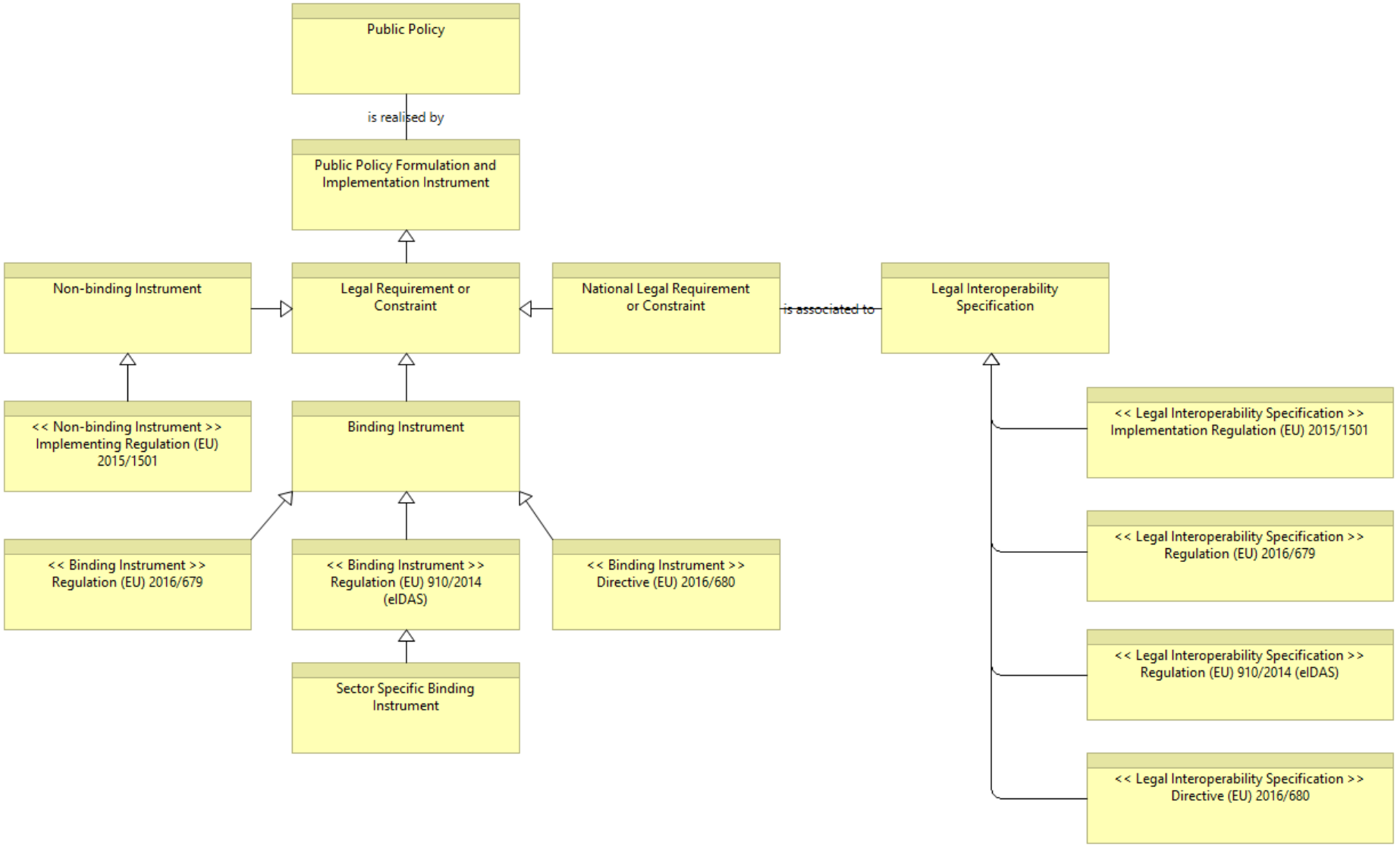
  https://ec.europa.eu/cefdigital/wiki/download/attachments/23003348/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf?version=1&modificationDate=1457112919000&api=v2

5 ACKNOWLEDGEMENTS

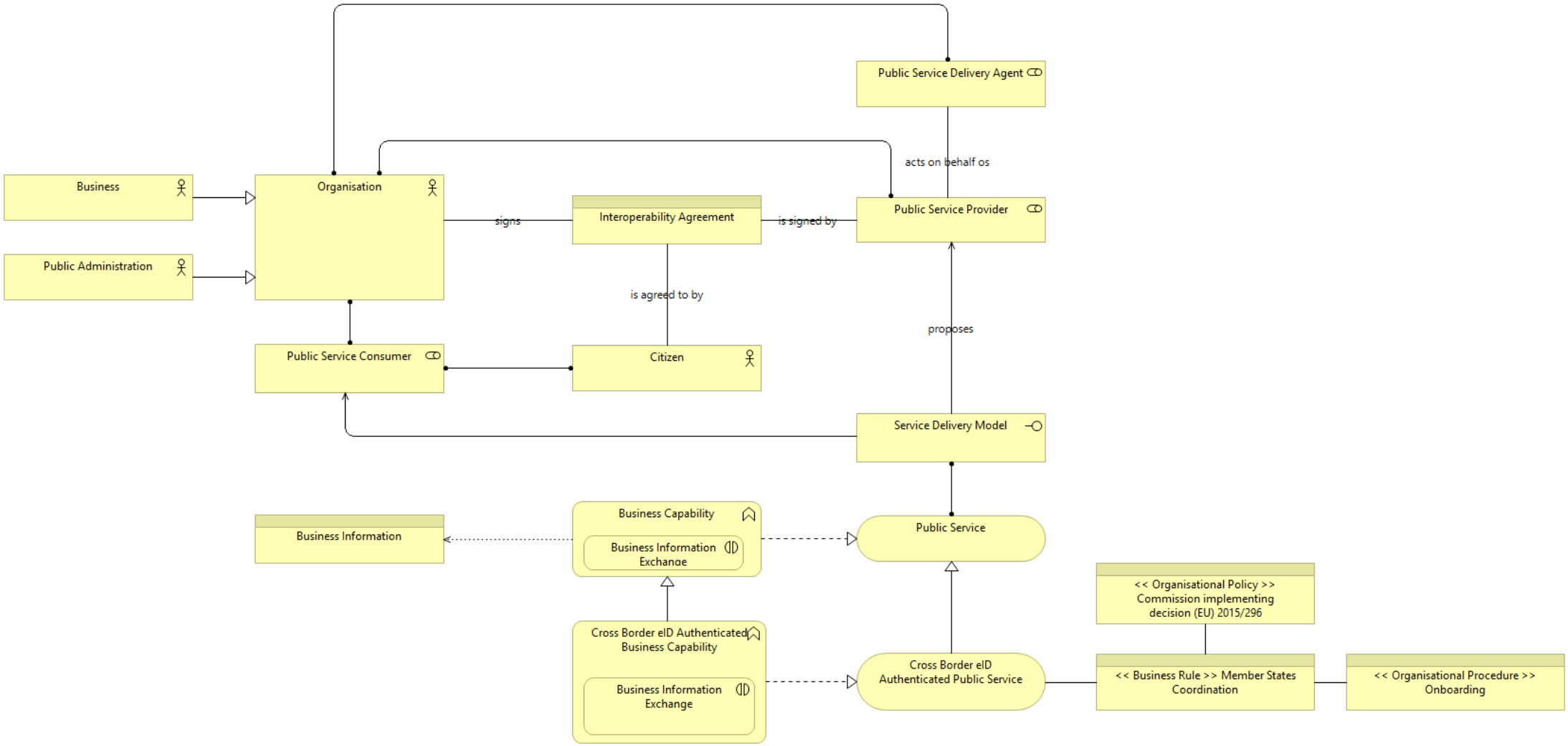
The creation of this SAT was made possible with the help of the EC DIG CONNECT and EC DIGIT B6. We would like to thank the following people for their input (alphabetical order):

- ALVARES RODRIGUEZ, Miguel
- CLOWES, Niel
- VASILESCU, Alice
- WIGARD, Suzanne

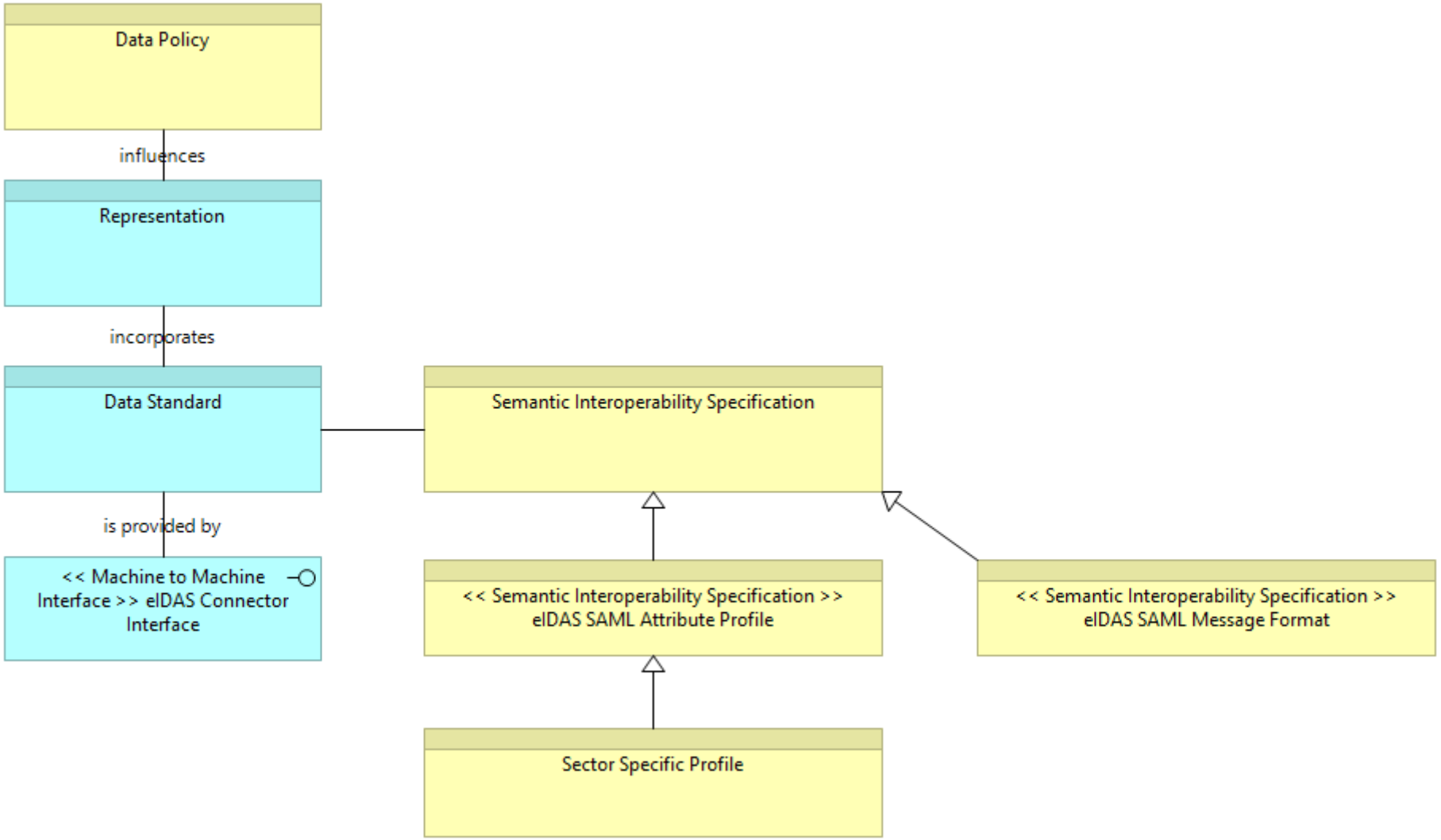
6 APPENDIX: LEGAL VIEW



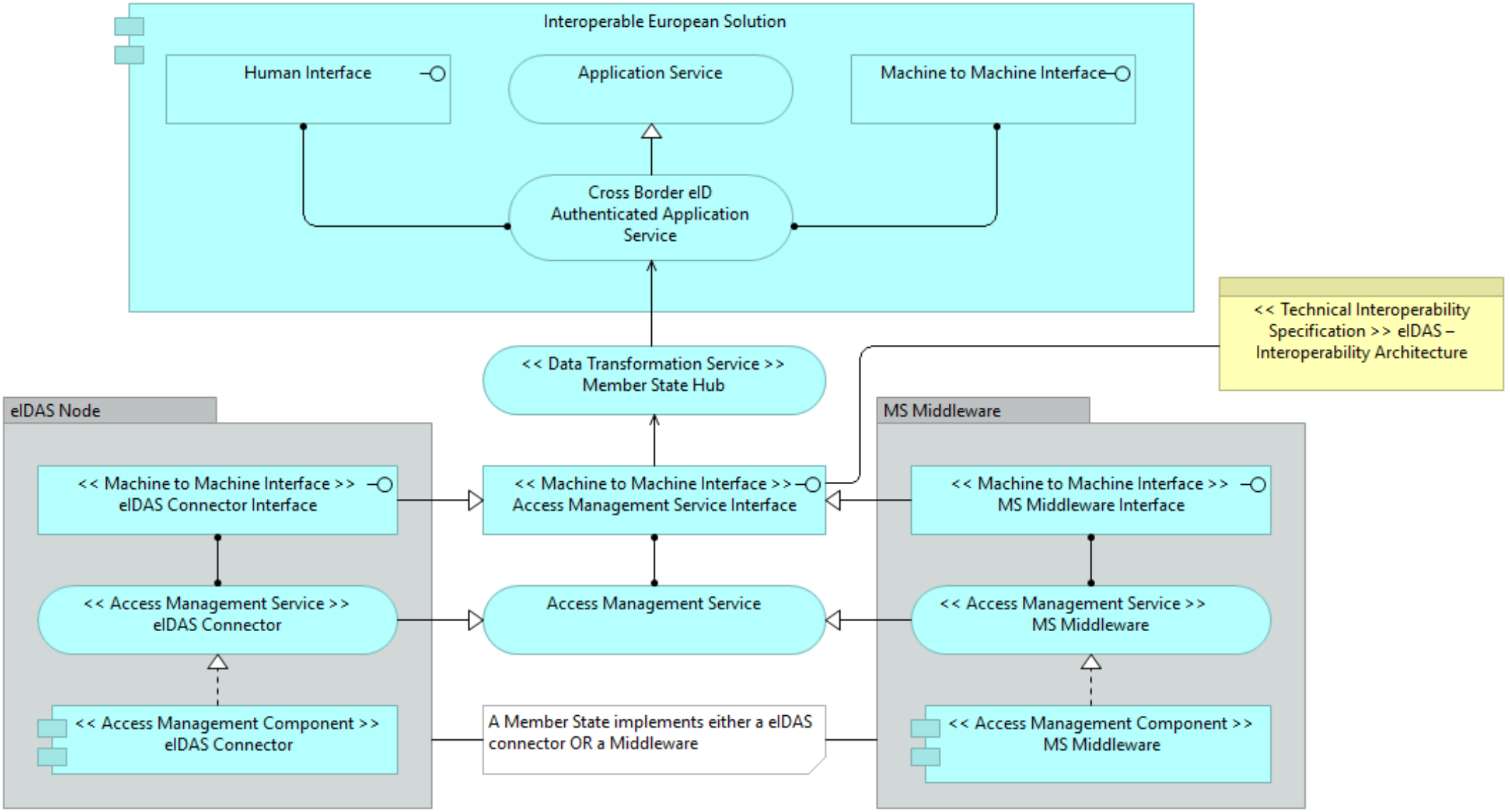
7 APPENDIX: ORGANISATIONAL VIEW



8 APPENDIX: SEMANTIC VIEW



9 APPENDIX: TECHNICAL VIEW – APPLICATION



10 APPENDIX: TECHNICAL VIEW – INFRASTRUCTURE