Submitted to the EC on 28/04/2017

COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME
ICT Policy Support Programme (ICT PSP)

Project acronym: e-SENS
Project full title: Electronic Simple European Networked Services
ICT PSP call identifier: CIP-ICT-PSP-2012-6
ICT PSP main theme identifier: CIP-ICT-PSP-2012-6-4.1 Basic Cross Sector Services
Grant agreement n°: 325211

D6.4 e-SENS European Interoperability Reference Architecture Evaluation

Deliverable Id :	6.4
Deliverable Name :	e-SENS EIRA Architecture Evaluation
Version :	V1.1
Status :	Final
Dissemination Level :	Public
Due date of deliverable :	10.4.2017
Actual submission date :	28.4.2017
Work Package :	WP6
Organisation name of lead partner for this deliverable:	JSI, LIST, AGID, eSPap, DTI
Editors:	Tanja Pavleska, Giorgia Lodi, Carmen E. Cirnu, Christian V. Rasmussen, Eric Grandry, Jörg Apitzsch, Klaus V. Pedersen, Pim van der Eijk, Massimiliano Masi, Herbert Leitold, Melis Demir, Giovanni Paolo Sellitto, Sander Fieten, Helder Aranha
Partners contributing :	Jozef Stefan Institute, AGiD, DIFI, Governikus, ICI Bucharest, LIST, DTI, Tiani Spirit, ARGE e-SENS.AT, Tübitak, ANAC, Chasquis Consulting, JM NRW, eSPap

Abstract:
This Deliverable is the final version of the Evaluation of the e-SENS EIRA and its artifacts.

History

Version	Date	Changes made	Modified by
0.10	10.03.2016	Initial version of the report	Klaus Vilstrup Pedersen
0.20	29.03.2016	Further updates	Christian Vindinge Rasmussen
0.30	10.04.2016	Setup of paragraph 3 and evaluation model	Christian Vindinge Rasmussen
0.35	18.04.2016	Inserted comments and additions from Carmen	Christian Vindinge Rasmussen
0.40	03.05.2016	More updates	Christian Vindinge Rasmussen
0.45	07.05.2016	Editorial changes	Christian Vindinge Rasmussen
0.46	11.05.2016	More editorial changes	Christian Vindinge Rasmussen
0.47	12.05.2016	Changes to paragraph 3 and 5	Christian Vindinge Rasmussen
0.48	12.05.2016	Editorial change to chap.5	Carmen Elena Cirnu
0.49	13.05.2016	Chapter 1 finalized; editorial changes	Klaus Vilstrup Pedersen
0.50	10.05.2016	Changes to chapter 5 and 6; editorial changes	Christian Vindinge Rasmussen
0.51	10.02.2017	Maturity Model and Security Model	Eric Grandry
0.52	20.2.2017	Methodology of Security Analysis	Tanja Pavleska
0.53	10.03.2017	eID Assessment	Herbert Leitold
0.54	13.03.2017	eDelivery Assessment	Pim Van der Eijk
0.55	15.03.2017	NonRepudiation Assessment	Massimiliano Masi
0.56	17.03.2017	Update to eDelivery Assessment	Pim van der Eijk
0.57	23.03.2017	eDocuments Assessment	Giovanni Paolo Sellitto
0.58	23.03.2017	Semantics Assessment	Giovanni Paolo Sellitto
0.59	22.03.2017	Update to Questionnaire Approach	Giorgia Lodi
0.60	26.03.2017	Update to Questionnaire Analysis	Giorgia Lodi
0.61	26.03.2017	Technical Maturity Model	Eric Grandry
0.62	27.03.2017	Pilots Security Analysis	Tanja Pavleska
0.63	28.03.2017	Trust Establishment Assessment	Jörg Apitzsch
0.64	29.03.2017	Review structure of assessment chapter	Eric Grandry
0.65	30.03.2017	Threat-based view on e-SENS security management	Tanja Pavleska
0.66	30.03.2017	Change figures of Pilots' Survey	Eric Grandry
0.67	30.03.2017	Mapping RMIAS to ENISA guidelines	Tanja Pavleska
0.68	31.03.2017	Restructuring of the Cybersecurity analysis	Tanja Pavleska
1.0.1.	05.04.2017	eDocuments and Semantics security	Giovanni Paolo Sellitto

		analysis	
1.0.2	06.04.2017	Cybersecurity Questionnaire in Annex IV and Summary of the security analysis	Tanja Pavleska
1.0.3	06.04.2017	EIRA Questionnaire template in Annex III, editorial changes	(several contributors)
1.0.4	10.04.2017	Editorial changes	Helder Aranha, Tanja Pavleska, G.P. Sellitto, Jörg Äpitzsch

Contributors

Name	Organisation	Country
Tanja Pavleska	Jozef Stefan Institute	Slovenia
Giorgia Lodi	AGID	Italy
Eric Grandry	LIST	Luxembourg
Helder Aranha	eSPap	Portugal
Massimiliano Masi	Tiani Spirit	Austria
Christian Vindinge Rasmussen	DTI	Denmark
Herbert Leitold	ARGE e-SENS.AT	Austria
Melis Ozgur Cetinkaya Demir	Tübitak	Turkey
Giovanni Paolo Sellitto	ANAC	Italy
Jörg Apitzsch	Governikus	Germany
Sander Fieten	Chasquis Consulting	The Netherlands
Pim Van der Eijk	JM NRW	Germany
Carmen Elena Cirnu	ICI Bucharest	Romania

Table of contents

List of Figures

List of Tables

Glossary

See: http://wiki.ds.unipi.gr/display/ESENS/Glossary

Executive Summary

The e-SENS project - Electronic Simple European Networked Services - aims at strengthening the Single Market by facilitating public services across borders. The previous Large Scale Pilots (LSPs) e-SENS builds on, STORK, PEPPOL, e-CODEX, SPOCS, epSOS, have already proven that the provision of electronic cross-border services is achievable and feasible. In numerous domains, technical Building Blocks have been developed and piloted, which enable seamless cross-border services addressing all the challenges faced and identified requirements. The Building Blocks developed in the previous Large Scale Pilots have been extended and consolidated during the e-SENS lifespan, industrialising the solutions and extending their potential to new domains.

e-SENS Work Package 6 - Building Block Provision aims to provide consolidated, re-usable building blocks for the implementation of digital services in Europe, supporting the overall goal of e-SENS.

As stated in the Technical Annex, the objective of evaluating e-SENS Reference Architecture (EIRA) and its artefacts is to:

- Support Transfer of Ownership and Operations through a knowledge transfer of Building Block state-of-play.
- Evaluate the Technical Maturity of the Building Blocks in relation to the Maturity Model in B.3 thereby contributing to an overall assessment of Building Block maturity.
- Evaluate the e-SENS EIRA in relation to Cyber Security.

This deliverable provides a structured evaluation of both the technical maturity and the security of the e-SENS Reference Architecture.

The **Technical Maturity assessment** relies on a maturity model customized for e-SENS Architecture, and structured around the concepts of *Solution Architecture Template* (SAT) and *Architecture Building Block* (ABB). A standardised assessment process operationalizes the model to evaluate each SAT of the EIRA. A survey has been conducted on the e-SENS domain pilots, in order to measure the technical maturity and collect the evidence. The outcome of maturity assessment shows that all SATs reach the reliability level, meaning their underlying specifications were thoroughly piloted through multiple implementations and that they are ready to integrate the design of specific solutions.

In addition, the pilot survey also contributed to the alignment of the Reference Architecture with the pilot solutions: a few gaps in specifications were identified and filled through EIRA change management process. Emerging solutions were also identified by the pilots and integrated into EIRA as generic building blocks (Non-Repudiation, Local Attribute Provision and Federated Signing).

The **Cybersecurity evaluation** relays on the adoption and extension of a standard security model, the *Reference Model for Information Assurance & Security* (RMIAS). This model serves as the foundation of a goal-based security analysis focusing on each SAT, assessing how the associated technical specifications contribute to meet the security goals. Besides this theoretical analysis, a survey was performed so as to collect the security practices deployed in e-SENS pilots. The outcome of this analysis shows that all pilots address an extended set of security goals, employing adequate means for their technical realization. However, the implementation of availability measures, proper risk analysis, and provision of human-oriented countermeasures requires better alignment with the specifications.

1. Introduction

1.1. Scope and Objective of Deliverable

The objective of this deliverable is to support the handover of Ownership and Operations and the transfer of the knowledge about the state-of-play of Building Blocks during the final period of the project, performing an evaluation of the e-SENS EIRA and its artefacts through:

- the evaluation of the Technical Maturity of the Building Blocks in relation to the Maturity Model in B.3 and thereby contributing to an overall assessment of Building Block maturity;
- the evaluation of the e-SENS EIRA in relation to Cybersecurity and perform a security analysis.

The main target group for this document are the stakeholders with key interest in the generic SATs and BBs from the e-SENS EIRA: it includes the CEF working group and the DGs of the EC that are active with setting up the CEF program. These are also the primary and only endpoint for the Transfer of Ownership and Operations of WP6, as stated in Deliverable 6.5. This document is also of interest for those organizations wishing to use e-SENS Building Blocks in their architecture (e.g. those developing solutions funded by the CEF program).

It is important to note that e-SENS building blocks (BB's) were not developed from scratch. Their design builds on results from previous LSPs, which in e-SENS were brought to their current state in terms of functionality and maturity, consolidated and deployed to new domains. Furthermore, they rely on already proven, mature, and relatively mainstream standards.

The previous work offered in general a strong basis for carrying out the work necessary to attain the objectives set by e-SENS, but it does not provide in itself a proof of the validity and suitability of what has been developed. Therefore, before the transfer of operations and ownership, WP6 carried out a technical assessment of the BBs produced or consolidated complementing the work done by the pilots and by WP3.

This work contains the results of the assessment process, both for the technical maturity evaluation and for an in-depth cyber security assessment.

1.2. Relations to Internal e-SENS Environment

The Architecture Evaluation Team of WP6 primarily collaborated with WP5-Piloting on setting the stage of how the pilot learnings can be incorporated in the Evaluation. The collection of information about the pilots has also required the contribution of WP5 experts.

WP3-Sustainability has also assessed the market maturity of e-SENS Building Blocks, focusing on the standardization of the Building Block specifications. The architecture evaluation reported in this deliverable is integrated within the global maturity model via the technical maturity dimension. WP3 furthermore has dependencies from D6.4 to their D3.7 where the sustainability assessment is made.

1.3. Relations to External e-SENS Environment

The primary purpose of this Evaluation is to align expectations on technical maturity with WP6 key stakeholder CEF, but also implementers of the e-SENS EIRA specifications and profiles, and target organizations for the sustainability of the e-SENS EIRA specifications and profiles.

1.4. Quality Management

The Architecture Evaluation Team has iteratively performed a complete evaluation of the EIRA, as reported in this deliverable. The WP6 team has reviewed the outcomes of the activities (design of the

technical maturity model and assessment process, pilots' survey questionnaire, maturity assessment of the building blocks, design of the cybersecurity model and pilot security questionnaire and cybersecurity assessment of the EIRA) during the WP6 plenary meetings, as well as via follow-up teleconferences.

The report itself (this deliverable) was produced by the Architecture Evaluation Team according to the quality standards of the e-SENS project, and it was subject to multiple review cycles within WP6. The process used to ensure the quality of the deliverable is summarized in **Table 1**.

Category	Remarks	Checked by
Conformance to e-SENS template	OK	WP6M
Language & Spelling	OK	WP6M
Delivered on time	OK	WP6M
Each technology description contains the correct elements	OK	WP6M
Consistency with description in the TA and in other e-SENS deliverables	OK	WP6M
Contents is fit for purpose	OK	WP6M
Contents is fit for use	OK	WP6M
Commitment within WP	Final remarks can be made in the 1st review cycle.	WP6M

Table 1. Quality checklist

1.5. Risk Management

This section summarises how the risks associated with the evaluation of the architecture have been managed by the Architecture Evaluation Team: risk identification, risk analysis, risk assessment and risk mitigation (**Table 2**).

Description	Prob.	Imp.	Prio.	Mitigation	Owner
Deliverable contains too much information, making it difficult to apprehend and maintain	High	High	High	Separation of concerns: - Textual report - Selective measures taken to ensure the right evaluation methodology	WP6
Feedback from pilots is scarce and technical maturity is hard to assess	High	High	High	Inclusion of experts from the pilot field. Integration of feedback from pilots. Explanation of the expected usage of the questionnaire to the pilot experts.	WP6

Table 2. Risk Management

1.6. Structure of the document

This report is structured according its main objectives:

- In chapter 2, the technical maturity model is defined, and the technical maturity of the building blocks is evaluated;
- In chapter 3, the evaluation of the EIRA from the cybersecurity perspective is addressed;
- Conclusions on the architecture evaluation are finally drawn in chapter 4.

2. Evaluation of technical maturity of Building Blocks

The evaluation of technical maturity of the building blocks requires the collection of information about the implementation and deployment of the building blocks specified in the EIRA: the feedback from the pilots is therefore of paramount importance to understand the effectiveness and comprehensiveness of the Reference Architecture.

This chapter is organised along the following 4 sections:

- Technical Maturity model: description of the adopted model and the assessment process;
- Pilot Survey: information gathering of pilots' usage through a questionnaire;
- Technical Maturity assessment of EIRA: use of the evidence collected from the pilots to assess the maturity of the EIRA components;
- Technical Maturity improvement: summary of the technical maturity evaluation results and recommendations to reach further levels.

2.1. Technical Maturity model

The methodology is an offspring of the maturity model defined in the Technical Annex. **Figure 1** sketches the overall maturity model and positions the technical maturity as one over 3 dimensions in the building block maturity profile: technical dimension (WP6), business dimension (WP5) and market dimension (WP3).

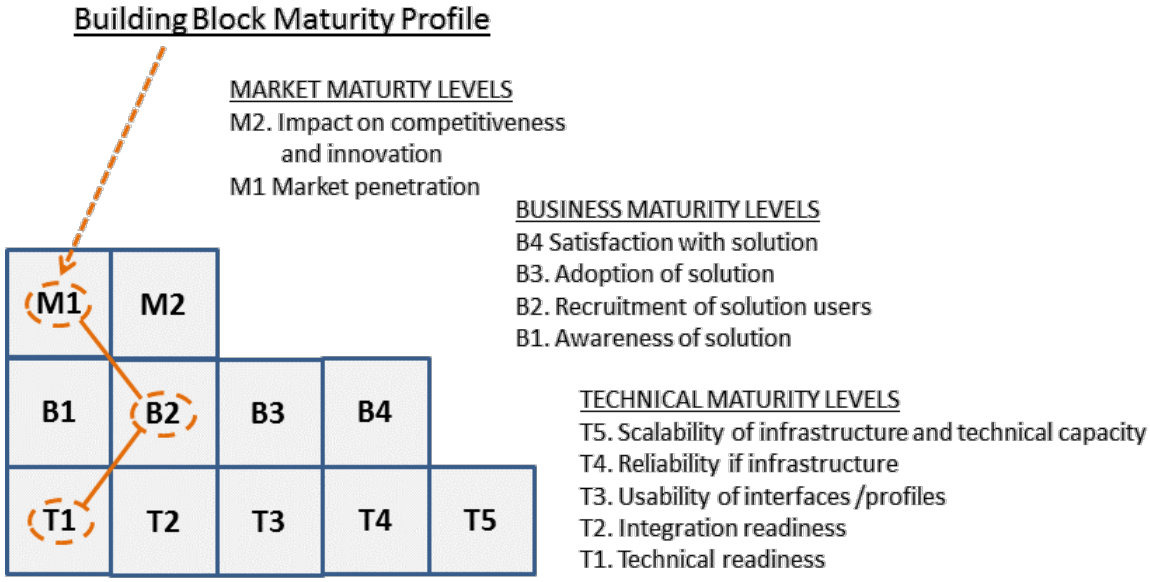

Figure 1. e-SENS Building Block Maturity model

The task for WP6 is to assess the technical maturity through reviews and test of ABBs and the SBB[1]s implementing the associated technical specifications. The different levels of Technical Maturity are

[1] Solution Building Block. For a more comprehensive description of EIRA see D6.7.

defined in the technical annex, and the Architecture Evaluation Team further elaborated this model into an actual assessment framework: the technical maturity assessment model. The model is based on the international standards in the domain of assessment, more specifically ISO/IEC 15504: the Capability Attribute captures which aspect of the building block is assessed (the meaning of each level), while the Practices associated with each level define how the assessment is performed (what is measured). The resulting technical maturity model is described in **Table 3**. It is worth indicating that the Solution Architecture Template (SAT) is the object of the maturity assessment: the SAT indeed combines Architecture Building Blocks (ABBs) to answer generic needs and as such is a template for the solution architecture to be designed.

Capability Level	Capability Attribute	Practices
1	Technical Readiness	Each required ABB Specification has been reviewed and approved by the Architecture Board. At least one SBB implementing a required ABB should exist that has passed the relevant conformance test and is documented.
2	Integration Readiness	The SAT has been reviewed by the Architecture Board. There is a documented set of SBBs implementing the required ABBs that has passed integration tests.
3	Usability Readiness	A set of SBBs implementing the required ABBs has been successfully deployed in a test pilot with the test results submitted and positively evaluated by both the Architecture and Domain Board.
4	Reliability Readiness	For each required ABB there exist multiple conformance tested SBBs. A set of SBBs which includes different implementation for each required ABBs has been successfully tested over a defined period of time.
5	Scalability Readiness	The SAT has been proven in a full-scale production environment.

Table 3. Technical maturity model

The maturity assessment process requires the evaluation of the Practices associated with each Capability Attribute according to a ***NPLF*** *rating scale*:

- **N**ot achieved (0 - 15%);
- **P**artially achieved (>15% - 50%);
- **L**argely achieved (>50%- 85%);
- **F**ully achieved (>85% - 100%).

The rating is based upon evidence collected against the practice indicators, which demonstrate fulfilment of the capability attribute. As most of the practices are associated with the implementation, testing and deployment of the ABBs, the evidence is looked for in the running pilots.

Next, the process of collecting evidence for the required assessment is explained with emphasis on the aspects relevant for the technical maturity assessment. This will allow filling in the necessary information in the table above for each EIRA SAT.

2.2. Pilot Survey

The e-SENS Reference Architecture (EIRA[2]) provides generic building blocks as a set of specifications and profiles to guide the definition of the pilots solution architecture and the implementation of the building blocks required in the pilots. Assessing the gaps between the reference architecture and the solution architecture is part of the EIRA evaluation, not only as an indicator of the reference architecture fitness-for-purpose, but also to assess the technical maturity of the EIRA according to the technical maturity model defined in the previous section. Hence, a pilot survey fulfils multiple purposes: (i) collection of evidences to support the technical maturity assessment; and (ii) gap analysis between reference architecture and pilot architecture, and especially the identification of emerging capabilities.

The pilot survey was run in the form of a questionnaire, which the Architecture Evaluation Team designed according to the structure of the EIRA and the concepts defined in the e-SENS Metamodel[3]. Specifically, it was organized in five main sections covering (i) the eService developed by the pilot, (ii) the business process realizing the eService, (iii) the Capabilities used from the Architecture Repository, (iv) the technical specifications plus solution implementation, and (v) general security and trust mechanisms. Additional questions cover conformance testing activities. The questionnaire template can be found in Annex III.

The questionnaire was answered by both collecting information from the Pilot Repository[4], and consulting experts actually involved in the development and deployment of the pilot solutions.

Due to project contingencies, the feedback of seven out of eleven pilots was collected close to the end of the project: WP5 indeed requested to only include the pilots that finalized the evaluation stage, i.e.:

- Citizen Lifecycle
  - NemKonto (run in Denmark and Spain)
  - eEducation (run in Sweden)
  - Patient Access (run in Austria)
- eHealth
  - ePrescription / Patient Summary
  - eConfirmation
- eProcurement
  - eTendering
  - Virtual Company Dossier (ESPD/VCD)

The answers to the questionnaire were analysed with a specific focus on the use of the BBs and their specifications, the use of security and trust mechanisms, and the conformance and interoperability testing activities: all mandatory information requirements to support the technical maturity assessment. The information provided regarding the business process is used to design an abstraction of the pilot architecture, bridging the solution architecture to the reference architecture.

Usage of ABB Capabilities

From the responses, it appears that eDelivery and eID are the most used SATs, with 4 out of 7 pilots adopting them. In contrast, Semantics is the least used SAT, deployed only in 2 of the 7 pilots. The eConfirmation pilot combines the highest number of SATs: only eID is not deployed in that pilot. At the

[2] http://wiki.ds.unipi.gr/display/eSENS

[3] http://wiki.ds.unipi.gr/display/eSENS/e-SENS+Metamodel

[4] http://wiki.ds.unipi.gr/display/eSENSPILOTS

opposite, the Nemkonto pilot (part of Citizen Lifecycle) only deploys the eID SAT. These statistics are presented in **Figure 2**.

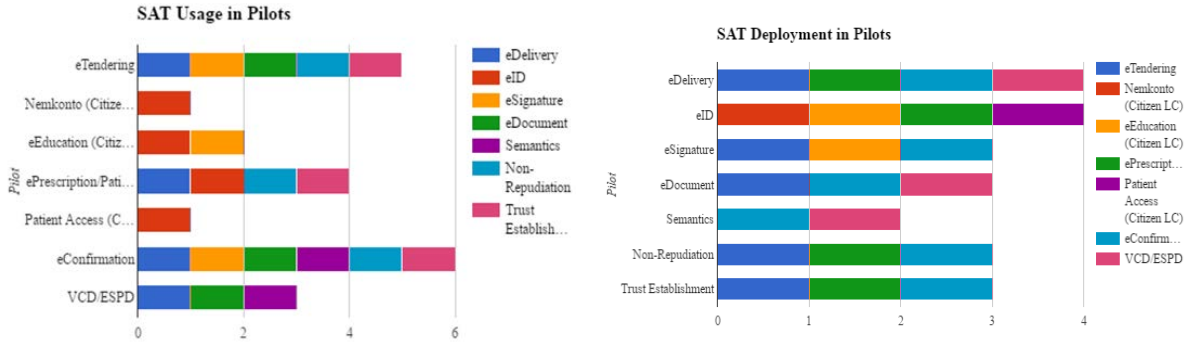

Figure 2. a) SAT Usage in Pilots; b) SAT Deployments in Pilots

Within the **eID SAT**, the ABB - Authentication Exchange is the main capability deployed in all the four pilots (as illustrated in **Figure 3**). At least two pilots have adopted the eIDAS specifications for Authentication Exchange. One pilot, the Citizen Lyfe Cycle (Citizen LC from now on) - Nemkonto in Denmark, is using the eIDAS implementation in one single node, i.e., in only one stakeholder, due to delays and issues with the produced code. The ePrescription/Patient Summary pilot has implemented and deployed the Local Attribute Provision capability in order to combine local authentication (through social security smart card) and remote authentication.

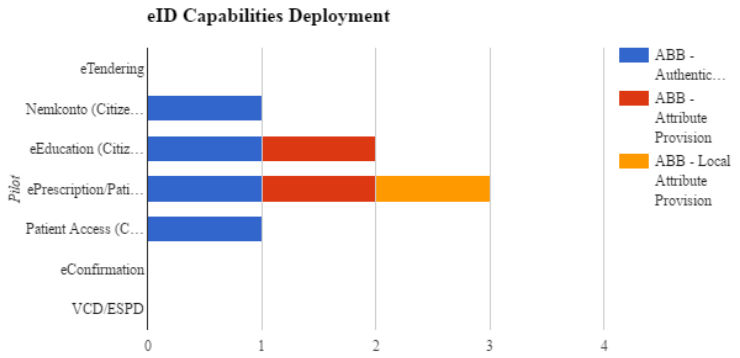

Figure 3. eID Capabilities Deployment

The **eDelivery SAT** is deployed in 3 of the analysed pilots (which apply the four-corner topology), deploying the e-SENS AS4 Profile as specification of Message Exchange capability (**Figure 4**). Two of these pilots also deploy Capability Lookup and Service Location capabilities, while the third one only deploys the Message Exchange capability. It is worth mentioning that the eHealth ePrescription/Patient Summary pilot makes use of Service Location and Capability Lookup capabilities to discover remote National Contact Points (NCP) capabilities and local private configuration information, without combining these capabilities with Message Exchange.

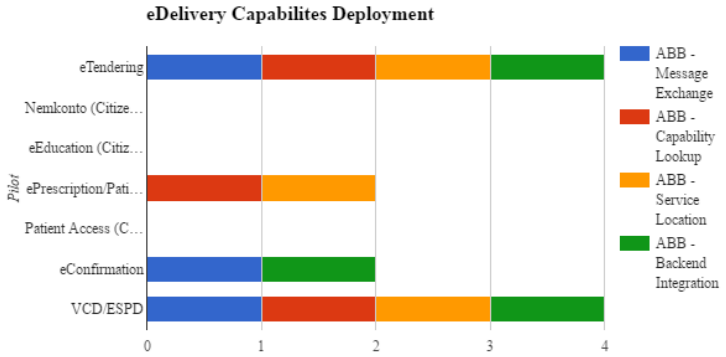

Figure 4. eDelivery Capabilities Deployment

As far as **eSignature SAT** is concerned, the Citizen LC - eEducation implemented a federated signing solution: this solution has been proposed and integrated into the e-SENS EIRA; 2 other pilots out of the 7 analysed realize specific solutions for electronic seals[5] management purposes: in the eTendering pilot, implementation activities are running in order to apply seals to payload on the ASiC-Manifest at Corner 1, to be validated at Corner 4 (end-to-end message source authentication). Finally, in the eConfirmation pilot, XML Advanced Electronic Signatures (XAdES) and PDF Advanced Electronic Signatures (PAdES) are used with X.509 certificates.

Three pilots out of 7 use the **eDocument SAT** and the ABBs that are part of it (**Figure 5**), with the exception of the ABB - Document Annotation that is not used at all. The main deployed capabilities are Document Provisioning, Document Packaging (and the ASiC Container specifications) and Document Routing (SBDH[6] specifications).

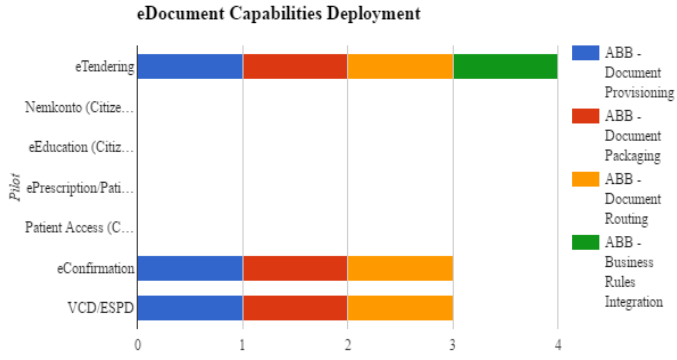

Figure 5. eDocument Capabilities Deployment

Only two pilots (eConfirmation and VCD-ESPD) deploy capabilities from the **Semantics SAT** (**Figure 6**). In particular, the ABB on ISA Core Vocabularies is employed in both pilots; however, domain-specific vocabularies are also envisaged as in the case of the eConfirmation pilot where documents are defined through UBL data core library and the business rules are defined in Schematron.

[5] Electronic seals are defined by Regulation (EU) No 910/2014 ("eIDAS"), in context of this document referred to as "seal".

[6] UN/CEFACT Standard Business Document Header

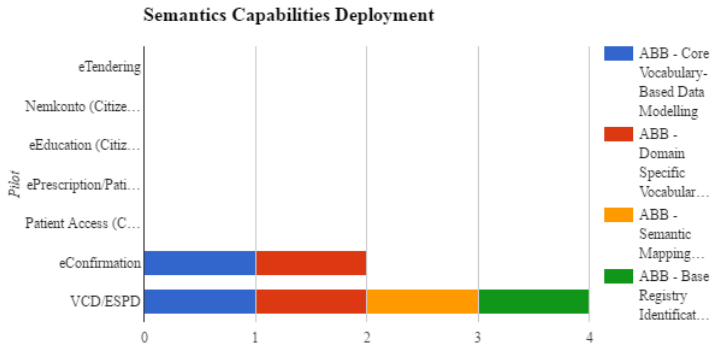

Figure 6. Semantics Capabilities Deployment

As for **Traceability SAT**, in the case of eTendering, REM delivery/non delivery evidence[7] is used when submitting a tender; in eConfirmation, the pilot that adopted the largest number of EIRA ABBs, a time stamping mechanism is implemented as a time service. It is worth mentioning that the Non-Repudiation ABB was first implemented in the eHealth pilot, and then integrated within the e-SENS EIRA as a generic ABB.

Finally, as far as the **Trust-Establishment SAT** is concerned, the most used solution is the Trust Network - PKI that is employed in the eTendering pilot, using the mechanisms developed in the context of the PEPPOL project, and in the eConfirmation pilot where verification of the seal is based on the exchange of public keys between the CIs and the Institution of the place of stay. This is also evident from **Figure 7**.

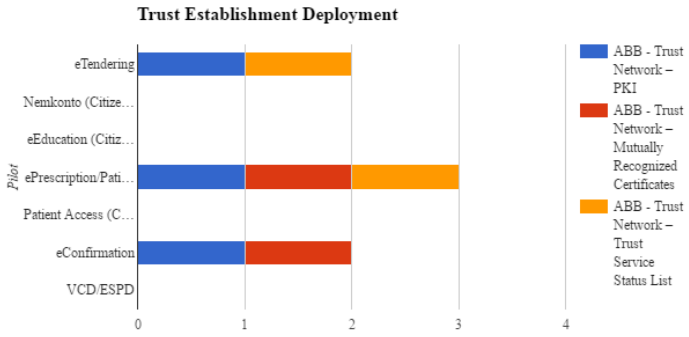

Figure 7. Trust establishment deployment

Usage of ABB Specifications

In order to identify possible gaps between what is described in the Reference Architecture and the actual use in the pilots, a set of questions on the actual usage of the specifications have been designed. The following findings emerge from the answers:

- the eIDAS specifications were employed with no issues in the Citizen LC - Nemkonto pilot;
- STORK specifications with some extensions were used in the Citizen LC - eEducation and in the Citizen Lifecycle - Patient Access pilots.
- the Non Repudiation ABB and its implementation made by the OpenNCP community contributed to meet the ePrescription/Patient Summary (eP/PS) pilot requirements, reducing

[7] Registered Electronic Mail evidence data format, as per ETSI TS 102 640-2.

implementation issues;

- all the ABBs profiles used in the eConfirmation and VCD/ESPD pilots met the pilot requirements.

Finally, the respondents identified the following gaps in the specifications and additional requirements for some of the seven pilots:

- for the Citizen Lifecycle - Patient Access pilot it emerges the lack of notified eID and the requirement for the provision of sector-specific (i.e. health in this case) identifiers;
- for the ePrescription/Patient Summary (eP/PS) pilot, the PR-BDXL specifications are only partially followed due to their dependency of Addressing of Entities ABB: a change request was issued to the e-SENS EIRA, and the specifications were updated;
- for the Citizen LC - eEducation pilot, there is the need for a signature solution that does not rely on DSS: a federated signing solution was designed, which has been reviewed by the Architecture Board and integrated into the EIRA;
- in the case of the Citizen LC - Nemkonto pilot, a SAML proxy was built in order to properly control the connection of the eIDAS node with the national infrastructure;

The feedback above has been integrated into EIRA through the Change Management process in place[8].

Security and Trust

From the responses to the questionnaire regarding the seven pilots that were analyzed, it emerges that information confidentiality mechanisms, as well as information integrity ones are used in most of them (**Figure 8**). Specifically, confidentiality mechanisms mainly involve encryption, with one pilot using encryption, password verification and security tokens. Information integrity principally involves hashing, file permissions and access control. In contrast, it is unclear whether information availability mechanisms are envisaged. Only in two pilots the scenario is clearer: Citizen LC - Nemkonto and VCD/ESPD do not use any of these mechanisms.

In all the analysed pilots the earlier mentioned mechanisms are not used to counter specific cyber threats: basically the pilots rely on the specifications as far as security is concerned. A detailed analysis of the cybersecurity is provided in section 3 of this report.

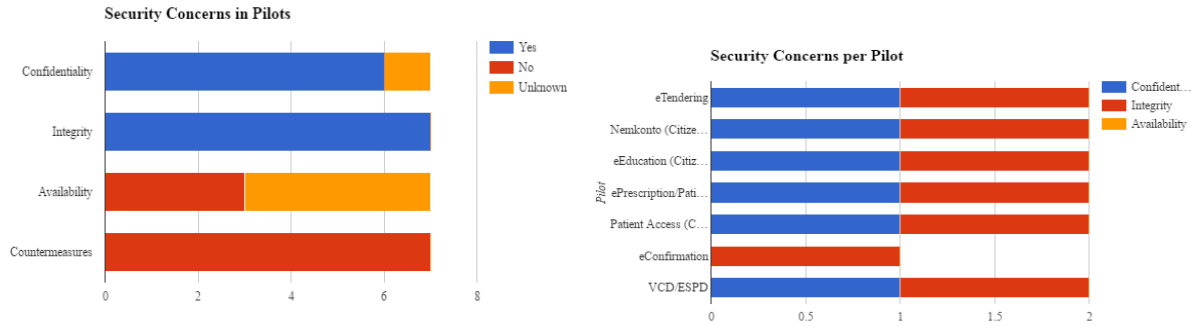

Figure 8. Security concerns in Pilots

Conformance and IOP Testing

This section of the questionnaire aimed at gathering information on the conformance and

[8] See D6.7, Section on EIRA Life-Cycle Management

interoperability (IOP) testing activities of the pilots that used e-SENS SBBs.

From the answers, one can draw the following scenario:

- In the context of the eTendering pilot, many open source and commercial products were conformance tested against the implemented AS4 Profile specifications and the BDXL specifications. Moreover, the interoperability between the products has been tested. In particular, IOP tests dubbed "Connectathons" were carried out with all tendering systems in the pilot with a monthly frequency;
- for the Citizen LC - Nemkonto pilot, testing activities involving the reference Implementation from DIGIT (eIDAS Node, relying on the eIDAS SAML Profile) were performed;
- in the Citizen LC - eEducation pilot, conformance and interoperability testing activities were carried out mainly for eID ABBs using STORK 2.0 specifications and infrastructure. Additional tests regarding eSignature were performed;
- in the case of the Citizen Lifecycle - Patient Access pilot, conformance and testing activities mainly involved STORK 2.0 eID and eIDAS BBs. Tests were performed between one service provider (Austrian “EMS”) and one foreign country identity provider (Denmark). The goal has been reached, since the interoperability tests were made among service providers coming from four different countries. In particular, the pilot tested the possible integration between the Austrian epidemic surveillance register EMS (“Epidemiologisches Meldesystem”) service and the eID building blocks;
- the eConfirmation pilot completed a connectivity test in the test environment. Both inbound and outbound scenarios were tested.
- in the *VCD/ESPD* pilot interoperability testing activities were performed for Holodeck and Flame Message Server.
- eHealth pilots (eConfirmation and ePrescription/Patient Summary) have organised several IOP testing events (“Connectathon”, “Expandathon”) during which the integration of several BBs has been tested, and more specifically the SMP/SML and Non-Repudiation.

Findings

All EIRA building blocks were deployed in the pilots, and the level of specifications is considered to be usable for implementation. A few issues were identified, and required either a change in the EIRA, or a change proposal submitted to the responsible standard development organisation (SDO).

Some building blocks were not initially defined in the EIRA, and emerged from the domain pilots:

- Non-Repudiation was first designed and implemented in the eHealth pilot; after successful testing, it was proposed to the Architecture Board and integrated within the EIRA;
- Local Attribute Provision was also first designed and implemented in the eHealth pilot; although it is currently dedicated to the eHealth domain (reading social security card), its potential for re-use has convinced the Architecture Board to integrate it within the EIRA;
- Federated Signing was initially a specific solution to eSignature in the Citizen Lifecycle pilot; it was proposed to the Architecture Board and included in the EIRA.

The pilots have not deployed countermeasures targeted towards specific threat-cases as part of the security mechanisms, and mainly rely on the security aspects of the technical specifications constraining the building blocks. A detailed analysis and assessment of the information security was performed by the Architecture Evaluation Team and reported in section 3.

2.3. BB Technical Maturity Assessment

The information collected through the questionnaire and analysed by the Architecture Evaluation

Team represents the knowledge base where evidences can be found when measuring the practices associated with each technical maturity level.

The assessment of the **eDelivery SAT** is restricted to its three ABBs: Message Exchange, Service Location and Capability Lookup. The Backend Integration ABB is not taken into account, as it is an abstract ABB for which no specification is provided and to which the concept of conformance testing therefore does not apply. Only the Message Exchange Building Block is required since Service Location and Capability Lookup are not used in the exchanges involving preconfigured configurations. A specification is provided for all three ABBs including Service Location (based on OASIS BDXL), but conformance tests are only provided for the specifications for Message Exchange (a profile of AS4) and Capability Lookup (based on OASIS SMP).

eDelivery SAT		
Level	**Assessment (N, P, L, F)**	**Evidence**
T1	F	For SBBs, see the column "SBB" in the section "SAT eDelivery" in http://wiki.ds.unipi.gr/display/eSENS/ Conformance test results for SBBs implementing the ABBs are documented in the "Software" section on https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Services
T2	F	The eDelivery SAT has been approved by the Architectural Board. Each of the three ABBs has been integrated successfully in at least one pilot environment.
T3	F	For each of the three ABBs, a conformant SBBs has been deployed successfully and evaluated positively in at least one e-SENS pilot.
T4	F	The conformance test result page lists eight conformant implementations of the ABB Message Exchange, which is the only required ABB. At least three of these implementations have been deployed and used successfully in at least one e-SENS pilot for one year or more.
T5	P	None of the e-SENS pilots using e-SENS eDelivery qualifies as "full scale production" as most are executed in test environments. In e-CODEX and EUCEG the Message Exchange ABB is deployed in production environments, but the volume of messages is still low. Also the Service Location and Capability Lookup ABBs (based on the e-SENS specifications) are not deployed in a production environment.

Table 4. Technical maturity assessment of eDelivery

The eDelivery SAT fully reaches reliability readiness (T4), especially thanks to the conformance testing campaign run both by the e-SENS Conformance Testing Team and the CEF eDelivery Team: the Message Exchange ABB and its associated AS4 Specification Profile have been implemented in multiple commercial and open source products, and deployed in several pilots.

In the area of **eID SAT**, e-SENS originally started based on the STORK 2.0 eID. In the course of the project this has been superseded by eIDAS eID, which is based on STORK 2.0 and developed the protocols and solutions further. As this evolution to eIDAS is also reflected in the e-SENS project results, like in piloting, as well as eIDAS being considered the sustainable path of a European eID infrastructure, the evaluation focused on the eIDAS solutions used by e-SENS.

eID SAT		
Level	Assessment	Evidence

	(N, P, L, F)	
T1	F	The eIDAS technical specifications for cross-border authentication and cross-border attribute provision have been finalised and approved by the Cooperation Network. SBBs passing the CEF conformance test regime are e.g. the AT and ES eIDAS nodes
T2	F	Integration tests of SBB implementations preceding pilot deployment include the CEF eIDAS node version 1.0 and 1.1 and national eIDAS nodes (like AT, DE, IT, PT, SE and DK). This is complemented by integration tests using the e-SENS eIDAS/STORK plugin to bridge from STORK 2.0 to eIDAS (like by IS and GR)
T3	F	Deployment in the pilots has been successfully carried out including different national eIDAS nodes as SBB implementations like by AT (eHealth Pilot involving Patient Access, Summary**,** and eAgriculture involving Citizen Services), PT, GR, IT (in eHealth pilot for Patient Summary), DE and NL (both in Citizen Services - eAgriculture), DK (Citizen Services use cases NemKonto and Patient Access), or IS (Record Matching).
T4	P	CEF conformance test regime has been positively completed for the ES eIDAS nodes (12/2016) and the AT VIDP (02/2017). SBBs have been deployed in the pilots (see above). The relatively short piloting period of a few months and the limited user constituency do however not yet justify a rating successfully tested over a defined period of time.
T5	N	While national eIDAS node implementations are based on and deployed in production environments (like the AT VIDP), this does not include production cross-border cases. Hence, no full-scale production environment can yet be claimed.

Table 5. Technical maturity assessment of eID

The eID SAT partially reaches reliability readiness (T4): its main ABB Capability (Authorization Exchange) is implemented in several SBBs according to the ABB Specifications, which have successfully passed the conformance tests. Moreover, these SBBs were deployed in several pilots. The change of strategy (from STORK 2.0 to eIDAS) during the lifetime of the project prevented from thoroughly piloting the SAT on a longer period.

Non-Repudiation SAT		
Level	Assessment (N, P, L, F)	Evidence
T1	F	The Non Repudiation technical specifications have been reviewed by the architectural board, and they can be found in the Architecture Repository. The ABB has been implemented, is available in https://ec.europa.eu/cefdigital/code/projects/EHNCP/repos/ehealth/browse/e-sens-non-repudiation and conformance tested by both Minder and Gazelle (test results are available on http://gazelle.ihe.net)
T2	F	The Non-Repudiation SAT has been reviewed by the Architecture Board. It has been implemented by different organizations (DIFI, University of Piraeus, OpenNCP) and used in pilots. At least 5 member states and additional non e-SENS member states, tested it with the Gazelle during at least three international testing events (http://gazelle.ihe.net)
T3	F	Deployment in pilots has been demonstrated in the "*eHealth simulated encounters*" (testing events with stakeholders) in June 2016 (AT-PT) and in October 2016 (AT-PT-ES). Test results have been submitted to the Architectural and Domain Board.
T4	L	The OpenNCP implementation has been conformance tested and piloted over 1 year of

		time by 4 member states (IT, AT, PT, ES).
T5	N	It is foreseen that eHealth will enter into production environment in 2018.

Table 6. Technical maturity assessment of Non-Repudiation

The Non-Repudiation SAT largely reaches reliability readiness (T4): the relevant ABBs have been implemented in multiple software solutions and conformance tested against the associated technical specifications. They were deployed in several pilots and tested during the e-SENS lifespan. Moreover, the eHealth pilot has pushed the implementation to be integrated in the OpenNCP Platform, to be deployed in production in 2018.

eDocument SAT		
Level	Assessment (N, P, L, F)	Evidence
T1	F	The eDocument technical specifications have been reviewed by the Architecture Board, and are available in the Architecture Repository. An eDocument engineering methodology has been defined by ISA in the Guidelines for public administrations on eDocument engineering methods and e-SENS Document Provisioning BB builds on these guidelines. eDocument Packaging is based on ETSI specifications ● ASiC Specs ETSI TS 102 918 V1.1.1 (2011-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC). ● ASiC Profile ETSI TS 103 174 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile . Conformance to an eDocument format can be verified using a Schematron, Business Rules can be verified with a Business Rule Engine (BRE) following the W3C Rule Interchange Format (RIF)
T2	F	The eDocument SAT has been approved by the Architectural Board. Four out of five ABBs (Document Routing - Packaging - Provisioning - Annotation - Schematron Rules) were successfully integrated in at least one pilot environment. eDocument Annotation is not explicitly used in Pilots, but the specification is used to store eSignatures in the container along with the signed documents; the specification is based on the Open Annotation (OA) Data Model described by W3C Open Annotation Community Group
T3	F	A set of SBBs compliant with the specification was deployed successfully in Pilots; namely, solutions based on ASiC containers and UN/CEFACT SBDH.
T4	F	For each ABB there exist multiple conformance tested SBBs, used in different Domains. eDocuments engineering guidelines have been adopted in e-SENS pilots, but also by Administrations outside of the project; the deployment of SBDH implementation was already successfully tested in PEPPOL Infrastructure over a long period; the ETSI container has been adopted in e-SENS pilots and tested during the lifetime of the project.
T5	P	The ESPD/VCD in Marketplaces pilot adopts e-SENS eDocument SAT and it is going to be deployed in a large-scale operational environment. At the time being, other e-SENS pilots are not reaching a widespread market implementation.

Table 7. Technical maturity assessment of eDocument

The eDocument SAT largely reaches reliability readiness (T4): the relevant generic ABBs (eDocument

Packaging and eDocument Routing) were implemented and deployed in multiple pilots and conformance tested against the associated technical specifications. Moreover, the ESPD/VCD in Marketplaces has adopted the e-SENS eDocument SAT and will deploy it in production.

Semantics SAT		
Level	Assessment (N, P, L, F)	Evidences
T1	F	The Semantics technical specifications have been reviewed by the Architecture Board, and are available in the Architecture Repository. Additional specifications can be found on ISA^2 website and Joinup. The access to base registries has been analysed in the context of the community in Joinup: https://joinup.ec.europa.eu/community/abr/home The core vocabulary named "Core Criterion and Core Evidence Vocabulary", developed in order to meet the objectives of the ESPD/VCD pilot, is described at the following URL: https://joinup.ec.europa.eu/asset/criterion_evidence_cv/description As for Domain-specific vocabularies, specialized standard data models are considered such as UBL for e-Procurement and Business Lifecycle and HL7 for e-Health: https://docs.oasis-open.org/ubl/os-UBL-2.0/UBL-2.0.html
T2	F	The Semantics SAT was approved by the Architecture Board. The VCD pilot has deployed all the Semantics ABBs; eConfirmation has deployed Core Vocabularies and Domain Specific Vocabularies. Besides these 2 pilots, Domain Specific Vocabularies are deployed in all pilots for message header and content engineering and processing, although they are not considered as generic ABBs. The concept of base registry is at the foundation of the trusted sources of information that are accessed in the pilots, even if it is not recognized as such.
T3	L	A set of SBBs compliant with the specifications were deployed successfully in various pilots: Semantic Mapping ABB is at the base the ESPD and e-Certis; Core Vocabularies compliant with the specifications are used in more than one pilot. The usage of domain specific vocabularies is still to be recognized (e.g. UBL 2.0 and SBDH)
T4	L	For each building block there exist multiple specifications and SBBs, at times hampering semantic interoperability
T5	P	Core vocabularies gained ground in the last years. An ISA action supports access to base registries Semantic Mapping is used in e-Certis (currently operated by DG GROW as part of the EU digital infrastructure and leveraged in the e-SENS VCD pilot as a trusted source of information) and in the VCD pilot. It was however difficult to make the pilot recognizing the use of semantics except in the case of VCD. A full market adoption is still to come.

Table 8. Technical maturity assessment of Semantics

The Semantics SAT largely reaches reliability readiness (T4): the relevant generic ABBs were implemented and deployed in multiple pilots and conformance tested against the associated technical specifications. Some relevant Domain Specific Languages, like UBL are widely adopted by the market, at the point that their usage is transparent to the user's community. Semantics is however still considered as complex to integrate and deploy, and only a few pilots have actually reached the benefits

associated with the usage of the Semantics SAT.

Trust Establishment SAT		
Level	Assessment (N, P, L, F)	Evidence
T1	F	Trust Establishment is achieved by means of well-adopted industry standards, in general ETSI ESI Standards for Certification Authorities and other Trust Service Providers are adopted by piloting domains according to their respective requirements. Basically PKI is used (e.g. OpenPEPPOL, CEF Digital Community PKI, controlled mutual key / truststore exchange) as well as Trusted Lists based on ETSI TS 119 612 v2.1.1. The eHealth domain uses an extended SMP model to trustworthy expose C1/C4 certificates, recently approved by OASIS as "Candidate Specification". Sample implementation is provided as CEF SMP V0.3 RC01 . The backbone of all Trust Models is conformance assessment and supervision of respective Trust Domain actors regarding the domain-wise defined policies and governance models.
T2	F	The SAT has been approved by the Architectural Board. Mostly, security and trust functionalities of runtime environments are used, which have a proven maturity for years already. Several added functionalities, like usage of Domain Trust List and SMP extended by exposure of C1/C4 certificates, have passed integrations tests.
T3	F	All the ABBs (conformant to specification) have been integrated successfully in several pilots; more precisely, eTendering (implementing PKI and Trust Service Status List), ePrescription/Patient Summary and eConfirmation implementing SMP in addition to the previous, etc. The Trust Network PKI is a widely used ABB in almost all of the domains, serving to establish either intra-domain or cross-domain trust.
T4	F(L)	F: Reliability has been proven for the related functionality provided by established PKI and runtime environments; this fact has been one of the main reasons to opt for them. L: Usage of verifiable, production-ready certificates by all actors still must be brought forward, as it has not been established for the PoCs of all piloting domains. In addition, maintenance and usage of Domain Trust List as well as extended SMP needs further testing. The Domain Trust List set up for eTendering requires additional policy refinement (content and interpretation of Trust Lists and their domain profiles, governance model to be established).
T5	F(P)	F: For security and trust means provided by established PKI and runtime environments. Used as such by most SATs. P: Applies for Trust List and extended SMP usage. Official MS Trust Lists are still about to be extended to cover all Trust Services as addressed by eIDAS. Domain Trust Lists, T5 maturity differs per piloting domain having set up such a TL. Extended SMP is implemented, successfully tested in the eHealth domain, currently between two countries (PT and AT).

Table 9. Technical maturity assessment of Trust Establishment

The Trust Establishment SAT fully reaches scalability readiness (T5). It is however worth emphasizing that the situation is slightly different for Domain Trust List solution, compared to the established PKI solution. Domain Trust List however largely reaches reliability readiness (T4), especially lacking extended testing.

2.4. Technical Maturity Improvement

Table 10 summarizes the technical maturity level per SAT. All SATs either largely or fully achieve level T4 - Reliability Readiness: the specifications they rely on have proved to be reliable by the e-SENS pilots, and they are therefore ready to be used to design and build specific solutions.

Technical Maturity	eDelivery	eID	Non-Repudiation	eDocument	Semantics	Trust Establishment
T5 - Scalability Readiness						
T4 - Reliability Readiness						
T3 - Usability Readiness						
T2 - Integration Readiness						
T1 Technical Readiness						

Legend:

Fully Achieved	Largely Achieved	Partially Achieved	Not Achieved

Table 10. Summary of technical maturity per SAT

As the uptake of the AS4 standard is already growing the maturity of the **eDelivery SAT** is further improved. But to reach full technical maturity also the Service Location and Capability Lookup ABB need to be implemented in large scale production environments.

Non-Repudiation SAT provides a full-scale solution if all its components (namely, PR-REM and/or PR-ATNA, PR-XACML, PR-PerHopProtocol, PR-EvidenceStorage) are deployed. However, in order that Non-Repudiation protocols perform well a governance model must be in place. A further improvement of this SAT is to provide compliant solutions for its specific realizations (e.g., Evidence Storage compliance with ISO-27037), and a "template" for a governance model that can be translated into XACML policies, to achieve irrefutable sequence of events. In addition, the PR-PerHopProtocol should be further studied with automatic tools (i.e., model checking).

Regarding the **eDocument SAT**, the Document Provisioning ABB may need further elaboration with regard to domain specific standards and their possible mapping to Core Vocabularies: some actions are already taking place in the context of ISA strategy, but we encourage further developments in this area. Document Routing ABB and its SBDH specification is in an acceptable stage of maturity and its adoption may help public administrations by providing a consistent interface between applications and improving possibilities for automated processing of documents. The Document Routing ABB and its ASiC specification is the most mature BB as it is based on international standardisation activities in ETSI. The BB has been piloted and is now running in various open source implementations, but its adoption should be fostered and encouraged in view of the deadlines for the adoption of the eIDAS regulation, since the ETSI container is purposefully developed to support the delivery and storage of detached signatures along with the documents, streamlining the process of mutual recognition of signatures.

Semantics SAT being the less deployed component of the architecture, was nevertheless implemented

in the eProcurement and Business Lifecycle pilots. These pilots share the common need to define mapping between typologies of documents that are required in business service related or e-Procurement procedures. The development of a Core Criterion Evidence vocabulary together with ISA has been a fruitful experience that can be supported as a best practice of consensus-making in a community-based environment. Core Vocabularies can become the basis of new context-specific data models or they can be mapped to context-specific data models that are already in use.

Usage of Domain Specific Vocabularies is recognized at an architectural level - pilots use the domain specific vocabularies and codelists as a heritage of previous LSPs. Further developments, translations and mappings in this area in view of a standardization work would improve a seamless cross-sector communication.

In the area of **Trust SAT**, mature standards are adopted and related infrastructure of runtime environments and PKI are used. The Domain Trust List and extended SMP models are however new concepts, in part recognized in the EFTA area only, but not yet adopted by the IT Industry[9]. The underlying specifications allow for domain profiling, which should be subject to another standardisation effort. Further systematic testing of implementations provided by e-SENS is required. Additional assessment/monitoring should be done by CEF in order to accelerate uptake and to improve reliability of these models and their implementations.

[9] This relates to Domain Trust List. Different from that, the Trusted Listed to be provided bei EUMS for the trust service providers addressed by eIDAS raise more and more international attention and support through solutions available on the market.

3. Evaluation of EIRA with respect to Cybersecurity

3.1. Background

One of the objectives outlined in the Description of Work of the project is to "*Evaluate the EIRA in relation to Cybersecurity*". This implies that a security assessment on an architectural level ought to be carried out.

Prior to initiating any debate on assessing the outcomes from the e-SENS WP6, i.e. of the ABBs and the SATs, it is important to note that these building blocks were not developed from scratch. Their design builds on previous results from other LSPs, which in e-SENS are being leveraged to their current state in terms of functionality and maturity, and further deployed to new domains. Furthermore, these components rely on already proven, mature, and relatively mainstream standards. A strong basis for carrying out the work necessary for meeting the objectives set by e-SENS was thus provided by the work on security and standardisation in general already performed by its sibling LSPs.

The fact that e-SENS is reusing the results from previous work that had addressed information security does not yet establish a convincing argument on having a sound security basis. Hence, the design and performance of the e-SENS components, as well as the e-SENS pilot preparation itself require their own security assessment when integrating results into a new operation whole in the pilot domains.

While thorough security analysis of the e-SENS piloting environment is helpful for the internal e-SENS's community, it would be less useful beyond e-SENS context. For example, future users that would plan on reusing the e-SENS building blocks would want to establish their own opinion of whether these components address the main information security requirements and risks their systems are exposed to in a certain domain. Support by e-SENS will be provided in that no exhaustive details about each of the component's descriptions or the security measures foreseen by a particular standard shall be needed. In that sense, a starting point on an architectural level about how information security has been addressed would be provided, as well as references to the actual details that would enable one to work out how the security requirements have been addressed.

The most useful way of perceiving e-SENS is through the "Lego brick metaphor" – as enabling new domains in using a set of building blocks according to their specific business needs. In doing so, some challenges will appear by the mere fact that EIRA operates on architectural level and that the building blocks serve various purposes and apply different standards or security solutions. This asks for a security evaluation methodology that is both applicable on architectural level and that presents security features in a uniform way for all of the building blocks. Thus, when new users aim to combine several building blocks into a solution, a common framework for expressing the security properties would also be in place.

The purpose of this evaluation is precisely to allow stakeholders who aim to build on e-SENS outcomes to get a quick overview of which security requirements have already been addressed by a particular building block. The methodology for meeting this goal is further elaborated in the next section.

3.2. Methodology

The main purpose of security evaluation on EIRA level is to communicate to the future users of the e-SENS results how critical aspects of information security were addressed in the project. The result is thus a common way to express the evaluation for all of the EIRA building blocks. It shall also support a domain employment of (a combination of) several building blocks, i.e. a solution requiring security assessment of several building blocks being incorporated into a single operational whole.

Given the heterogeneity of the different building blocks and the fact that they serve different purposes,

the methodology that was chosen builds on two common denominators: on the one hand, core information security objectives that are general enough to address all domain needs are desirable; on the other hand, they should be applicable to the SENS cross-border architecture, and more specifically to both eDelivery and eID cross-border architectures.

In order to reach these objectives, a commonly agreed model of information security is adopted: the **Reference Model for Information Assurance and Security** (RMIAS).

The RMIAS identifies the following security aspects (dimensions) of the Information System: Life Cycle, Information Taxonomy (Classification), Security Goals and Countermeasures. Although it integrates the countermeasures dimension, the RMIAS is mainly aimed to support a goal-based security management, as "*focusing on goals allows security experts to communicate with other stakeholders using concepts that do not require technical knowledge* (RMIAS)". It is precisely this generality of the model that makes it adequate to the purposes of this analysis. The objectives and the results of e-SENS are meant to be communicated to a variety of stakeholders for whom a strong technical background should not be a prerequisite. Thus, the information must be easy to read for a non-technical person who would in most cases be unacquainted with formal security models or questions regarding security technologies.

In addition to modelling **security goals/objectives**, modelling **security risks/threats** can be regarded as equally usable since each addresses the others' main concern implicitly. In order to provide a holistic evaluation of EIRA with respect to security, a threat-based view on security management is also part of the analysis. With the RMIAS being complemented with a threat-based view on security, an extended reference model is obtained, as depicted in **Figure 9**.

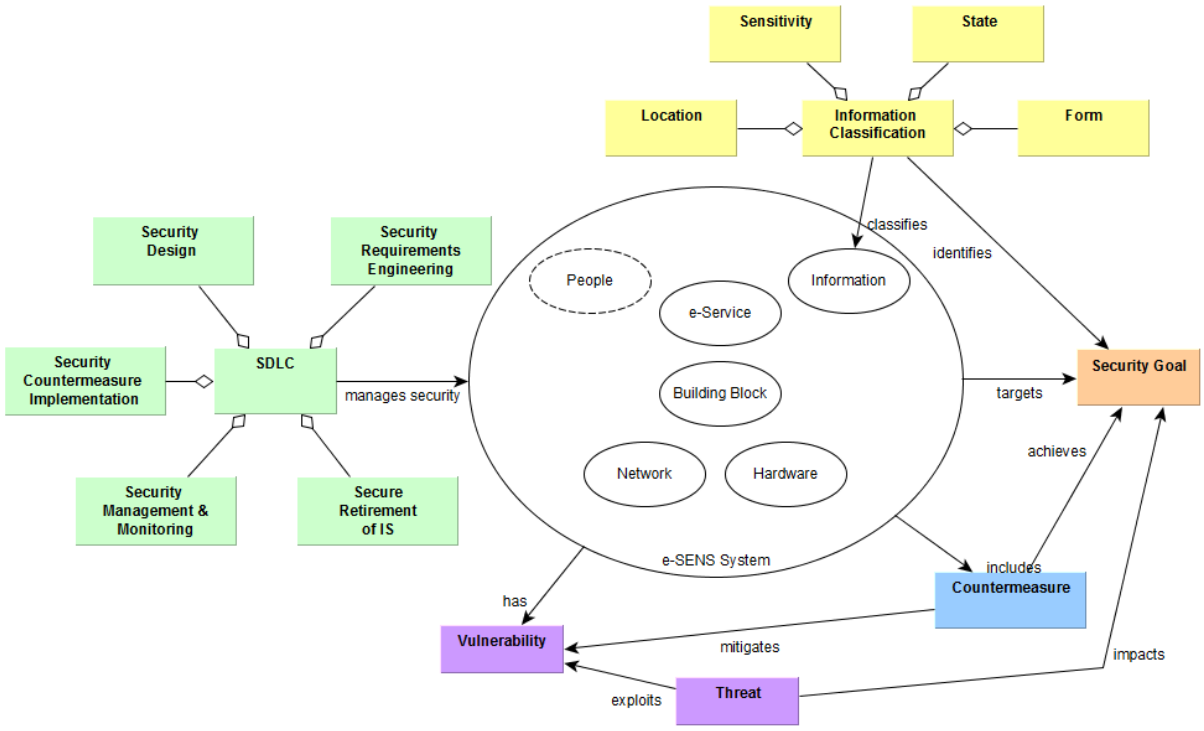

Figure 9. The extended goal-based approach

In the core of the extended model is the e-SENS System with all its assets. The different **security management** approaches are thus aimed at affecting and interacting with the e-SENS system.

The information classification helps to understand the relevant security goals associated with the eService System. The information is classified according to the following dimensions:

- *Form*: in e-SENS the information is exclusively manipulated in electronic form;
- *State*: the information manipulated in e-SENS can be in one of the following states: Creation, Transmission, Storage, Processing, Destruction;
- *Sensitivity*: the information manipulated in e-SENS can be either confidential, or non-confidential;
- *Location*: the information is manipulated in various locations (MS, shared infrastructure, end-entities), however all are controlled locations, i.e. under full control of an organisation.

The **security goals** investigated here are in essence the fundamental RMIAS security goals:

1. *Confidentiality*, the property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 27000:2016];
2. *Integrity*, the property of accuracy and completeness [ISO/IEC 27000:2016];
3. *Availability*, the property of being accessible and usable upon demand by an authorized entity [ISO/IEC 27000:2016];
4. *Accountability,* the property that enables activities on a system to be traced to individuals who may then be held responsible for their actions [NCSC-TG-004];
5. *Authentication (and Trustworthiness)*, the provision of assurance that a claimed characteristic of an entity is correct [ISO/IEC 27000:2016], which can be further divided into
    - data origin authentication (like with electronic signatures)
    - entity authentication (the process of electronic identification of a person);
6. *Non-repudiation*, the ability to prove the occurrence of a claimed event or action and its originating entities [ISO/IEC 27000:2016] (which can be further subdivided depending on the process like non-repudiation of creation, non-repudiation of receipt, etc.);
7. *Auditability,* i.e. the ability to perform an *audit,* defined as the systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled [ISO/IEC 27000:2016].

In addition to the main security goals, *Access Control* is also investigated in order to analyse whether a certain building block provides the proper security means that ensure access to assets is authorized and restricted based on business and security requirements [ISO/IEC 27000:2016]. Furthermore, *Privacy Controls* are analysed to examine whether measures are in place that treat privacy risks (by reducing their likelihood or their consequences) [ISO/IEC 29100:2011].

Note: *Availability* is not part of the BB's security evaluation, as it is considered as a more operational aspect that is irrelevant on architectural level. However, it is addressed in the analysis of the pilot implementations, which is presented in the next section.

The **threat and vulnerability view** of the model abstracts the attacks exploiting the security weaknesses of the system under analysis.

The **countermeasure view** of the model abstracts the security controls that are deployed to mitigate the security threats and vulnerabilities of the system and reach the security objectives.

The security model supports both goal-based and threat-based security assessment. In a goal-based approach, the security goals are first defined, and the countermeasures helping to reach these goals are then selected. In a threat-based approach, the threats and vulnerabilities of the system to be secured are analysed, and the countermeasures mitigating the threats and vulnerabilities are then selected. Both approaches can be combined coherently, thanks to the **extended model**, and more specifically the integration of the goal view and the threat view.

When considering the architecture of the system to be protected (high-level of abstraction), a goal-

based approach is usually deployed. A threat-based approach requires detailed analysis of the complete system vulnerabilities, and therefore knowledge of the detailed design of the system (including software, hardware, network and organisational processes). In addition, threat- or risk-based approaches are usually in need of statistics of former system behaviour or other data to thoroughly evaluate risks and vulnerabilities of a system. However, data like that is not available during the development phase of a system. Therefore, it is important to stress that the threat-based view is complementing the goal-based approach; the relevant information for the threat-based analysis is extracted from the concrete solutions (pilots) implementing the building blocks, according to the analysis provided in the next section.

The goal-based **assessment method** is performed as follows:

1. The architecture of the system to be protected is described, and the various stages of information manipulation are identified;
2. For each stage, the information manipulated is classified, according to the information view of the security model. The associated security goals are then deduced;
3. Each of the security goals are then analysed and catalogued in relation to the relevant architecture.

The e-SENS System can be abstracted in various ways: the architecture description (i.e. the e-SENS Reference Architecture) associated with each eService, the actual solution design, the organisation deploying the solution, etc. In the evaluation, we concentrate on the architecture description relevant to the various eServices. Based on the previous analysis of the employment of the building blocks in the pilots, we analyse the cross-border architectures that are most employed by the pilots while carrying the bulk of the security mechanisms: eID, eDelivery, Non-repudiation, Trust Establishment, eDocuments, and Semantics.

3.3. EIRA Security Analysis

3.3.1. SAT eID

The eID architecture was originally based on STORK and STORK 2.0 work. This has meanwhile been superseded to a large extent by the eIDAS implementing acts and eIDAS technical specification. These are in particular the Commission Implementing Regulation (EU) 2015/1501 on the eID interoperability framework, the Commission Implementing Regulation (EU) 2015/1502 on Levels of Assurance (LoA), and the eIDAS Technical Specification version 1.1. Although some security aspects have changed from the original STORK and STORK 2.0 work, the current security evaluation is based on the latest eIDAS results; examples of such security-relevant changes from STORK to eIDAS are that SAML assertion encryption has been introduced by eIDAS, or that eIDAS introduced SAML metadata for the distribution of signer certificates and encryption certificates.

The eIDAS Architecture is represented in the **Figure 10**, where each eIDAS Node abstracts the integration of the MS-specific eID Components within the eIDAS Network.

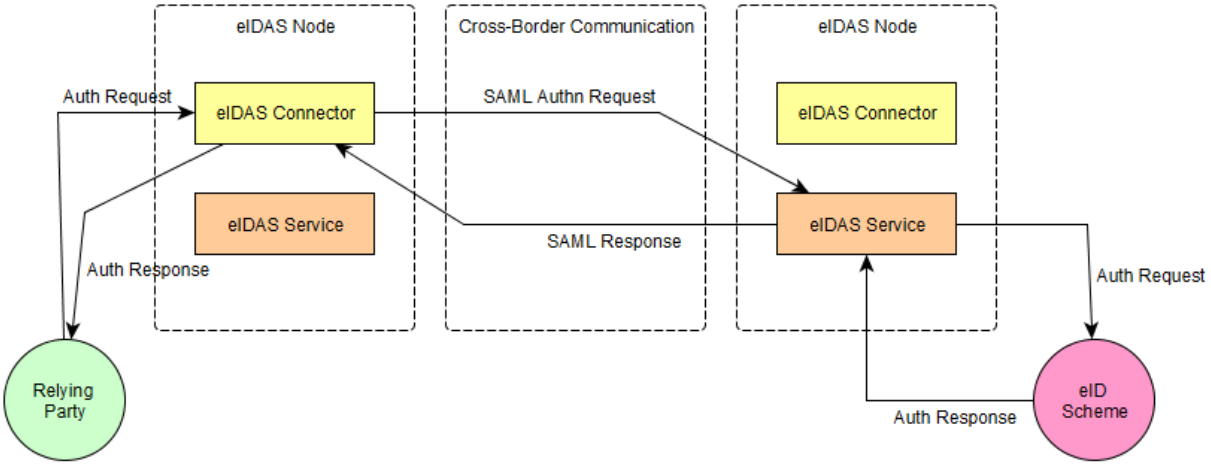

Figure 10. The eIDAS Architecture

Note that eIDAS does not interfere with how MSs implement their notified eID. LoA are defined in an output-oriented manner with only a few specific technical requirements. In the evaluation this is indicated by the remark «MS-specific», meaning that the security measures are not defined by e-SENS or eIDAS, but by the national eID scheme.

The security goals are set in relation to the eID Architecture, i.e. an "*Endpoint(1) → eIDAS Node (2) → eIDAS Node (3) → Endpoint (4)*" architecture, where the endpoint represents both the Relying Party and the eID Scheme. When investigating how security goals are addressed, the following vertices and edges are considered:

- Endpoint-eIDAS Node (1-2 or 3-4): This edge usually refers to the communication path under a Member State's responsibility, commonly denoted as intra-domain communication. We do not differentiate between the sending edge (1-2) and the receiving edge (3-4), unless otherwise stated, as the security measures of the building blocks are usually the same for both edges.
- eIDAS Node-eIDAS Node (2-4): This edge represents the cross-border (or cross-domain) communication path between two Member States, which is the core aspect e-SENS deals with.
- End-to-end security (1-4): While the eID Architecture is based on segmented trust relationships (1-2, 2-3, 3-4 each building a circle of trust), security relationships between the endpoints may be provided, like encryption for the final receiver by the original sender.
- eIDAS Node security (at (2) or (3)): Security goals may as well be fulfilled by the eIDAS Nodes, in store and forward components temporary encryption while data are at rest.

The eID mainly exchanges authentication request and response, exclusively in digital form.

Information	Sensitivity	Location	State	Security Goal
Authentication Request	Non-Confidential	Controlled	Transit	Integrity,
Authentication Response	Confidential	Controlled	Transit	Confidentiality, Integrity, Availability

Table 11. Information Classification for eID

For each identified vertex and edge, the security evaluation gives a reference to the specification and/or the standards that have been applied. Individual endpoint security – i.e. security measures at Node (1) or (4) – is not addressed, as it is not part of the e-SENS specifications.

Note that STORK as well as eIDAS support both centralised and decentralised deployment models that

Member States can choose at their discretion. If either or both the sending and the receiving Member State apply the decentralised deployment model, segmented trust relationships exist. End-to-end security between the person being authenticated and the relying party is provided if both Member States apply the decentralised deployment model.

eID SAT	End-point-eIDAS Node (1-2 / 3-4)	eIDAS Node-eIDAS Node (2-3)	End-to-End (1⇦4)	eIDAS Node (2) or (3)
Access Control	MS-specific [10]	n/a (eID is used over open communication networks)	n/a	ISO/IEC 27001 or similar for an eIDAS service (node (3)) [11]
Authentication	MS-specific	TLS server certificates on the communication link; EV certificates until 2017, qualified certificates from 2018.[12] SAML requests and SAML responses must be signed. [13] SAML signer certificates are published in SAML Metadata files that are signed by MS-notified certificates.[14]	MS-specific	For eIDAS node administration through ISO/IEC 27001 certification (see Access Control at gateways above)
Confidentiality	MS-specific	TLS with minimum crypto requirements.[15] Encrypted SAML assertions in the SAML response.[16]	MS-specific	n/a [17]
Integrity	MS-	Through signed SAML requests and SAML	MS-	n/a

[10] Security provisions of the notified eID depends on the MS implementations, eIDAS does not set technical requirements other than the LoA defined in (EU) 2015/1502. If, for e.g. the eIDAS SAML profiles are used on a national level, the same provisions apply as for the gateway-gateway edge (2-3).

[11] The interoperability framework (EU) 2015/1501 article 10.1 requires operation in an ISO/IEC 27001 (or equivalent) certified environment for eIDAS nodes providing authentication, i.e. the eIDAS service that asserts a notified eID. This includes restricting access to gateway administrative functions.

[12] See eIDAS technical specification v1.0, part „eIDAS - Cryptographic requirements for the Interoperability Framework - TLS and SAML“, section 2.4

[13] See eIDAS technical specification v1.0, part „eIDAS – Interoperability Architecture“, section 3.2.1 and section 3.2.2. The relevant SAML standard is the SAML Core specification “OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005”

[14] See eIDAS technical specification v1.0, part „eIDAS – Interoperability Architecture“, section 2.4 and section 6. The relevant SAML standard is the SAML Core specification “OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005”, as well as metadata standards “OASIS Committee Specification, SAML V2.0 Metadata Interoperability Profile Version 1.0, August 2009”, and “Metadata Profile for Algorithm Support Version 1.0”

[15] See eIDAS technical specification v1.0, part “eIDAS - Cryptographic requirements for the Interoperability Framework - TLS and SAML”

[16] See eIDAS technical specification v1.0, part „eIDAS – Interoperability Architecture“, section 2.4 and section 6. The relevant SAML specifications are “OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005”, “OASIS Committee Specification, SAML V2.0 Metadata Interoperability Profile Version 1.0, August 2009”, and “Metadata Profile for Algorithm Support Version 1.0”

[17] No personal data is stored by the eIDAS nodes, see Commission Implementing Decision 2015/1501 on the Interoperability Framework, article 6(2). Confidentiality of other information assets (e.g. access credentials or cryptographic keys) is an operational aspect covered by ISO/IEC 27001 certification or similar operational security provisions.

	specific	responses (see Authentication above)	specific	
Non-repudiation	MS-specific	Only provided at the very moment of an authentication via signed SAML responses (see Authentication above). No provisions for later evidence of a particular authentication on the gateway level, as logs may not contain personal data. [18]	MS-specific	n/a
Accountability	MS-specific	same as above applies: No provisions for later evidence of a particular authentication on the gateway level, as logs may not contain personal data.	n/a	ISO/IEC 27001 or similar for an eIDAS node
Auditability	MS-specific	n/a	n/a	For eIDAS node through ISO/IEC 27001 certification or similar

Table 12. Goal-based analysis of the eID SAT

3.3.2. SAT eDelivery

eDelivery is about providing secure and reliable electronic transfer of documents and data between organisations. In e-SENS, the focus for eDelivery is on cross-border data exchange. The eDelivery SAT uses a so-called *four-corner model* where parties are connected through Access Points. In this model only the message exchange between the Access Points is standardized. The way systems are connected to the Access Point is a decision made between the connecting party and its Access Point. **Figure 11** shows the e-SENS eDelivery architecture.

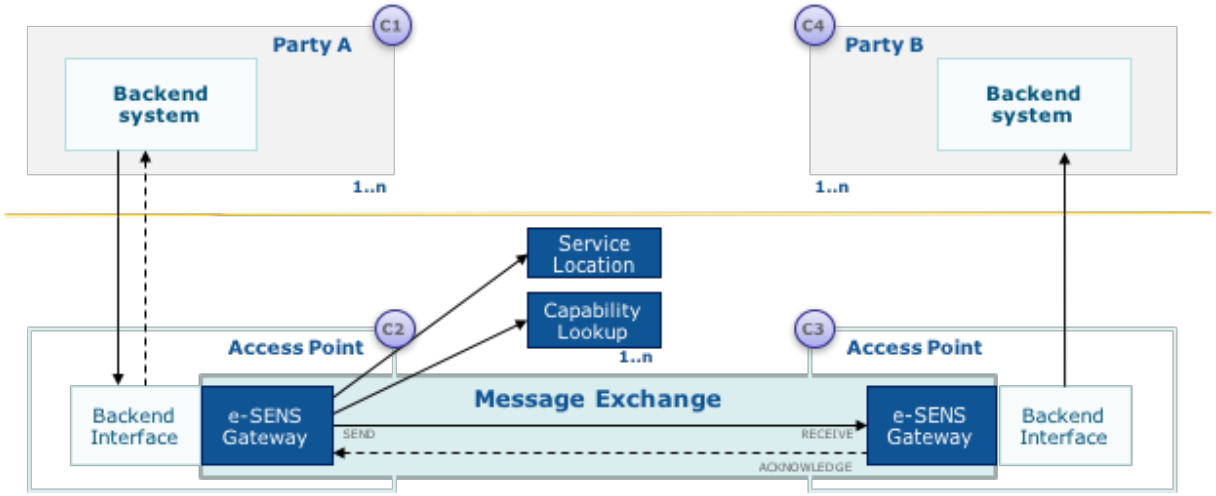

Figure 11. The e-SENS eDelivery architecture

As shown in the figure, the eDelivery SAT beside the Message Exchange ABB also includes the Service Location, Capability Lookup and Backend Interface/Integration ABBs. The first two ABBs are used to find meta-data about the parties connected to the network so the Access Point are able to set up the connection and perform the message exchange.

The Backend Integration ABB is abstract and implementation-specific and depends on the way the

[18] See Commission Implementing Decision 2015/1501 on the eID interoperability framework. Article 6(2) prohibits storing of personal data at eIDAS nodes, which would be needed as evidence for non-repudiation of an authentication process at later stages, only logging a subset of data to reconstruct a sequence of events is permitted under article 9(3).

Access Point is connected to the parties it serves, e.g. using another messaging network or directly over the internet. Therefore, this ABB is out of scope for this security evaluation.

For the evaluation of Information classification, information exchange is grouped in three categories: data/document exchange, service location and capability lookup.

The first of these categories can be subdivided in two sub-categories: electronic business documents and/or data exchanged between parties using message transfer; and Message Signalling information, which is information about the message exchanges. Two types of signals are Receipts and Errors.

The second and third categories can be subdivided in sub-categories for the location and capability requests and responses, respectively.

Information	Sensitivity	Location	State	Security Goal
eDelivery Message Transfer	Confidential	Controlled (eDelivery Infrastructure)	Transmission, Storage	Access Control, Authentication, Integrity, Confidentiality, Non-Repudiation, Auditability
eDelivery Message Signalling (Receipts, Errors)	Non-Confidential	Controlled (eDelivery Infrastructure)	Transmission, Storage	Authentication, Integrity, Non-Repudiation
eDelivery Service Location Request	Non-Confidential	Controlled (eDelivery Infrastructure)	Transmission	None
eDelivery Service Location Response	Non-Confidential	Controlled (eDelivery Infrastructure)	Transmission, Storage	Authentication, Integrity, Non-Repudiation
eDelivery Capability Lookup Request	Non-Confidential	Controlled (eDelivery Infrastructure)	Transmission, Storage	None
eDelivery Capability Lookup Response	Non-Confidential	Controlled (eDelivery Infrastructure)	Transmission, Storage	Authentication, Integrity, Non-Repudiation

Table 13. Information Classification for eDelivery

The classification of Sensitivity for business document/data exchange as Confidential does not preclude the use of eDelivery for exchange of non-confidential data or documents or signals.
All components used in eDelivery (Messaging Service, Metadata Location Service, Capability Service) may have additional interfaces that are not considered in the table above, for example for administration.
The classification of Service Location and Capability Lookup information as Non-Confidential reflects the use of these services in e-SENS pilots, where this information is non-confidential and available on the public Internet.
Table 14 summarizes the goals-based security analysis for eDelivery. References to specific versions of standards and specifications are provided in the e-SENS EIRA.

eDelivery SAT	C1-C2	C2-C3	C3-C4	eDelivery Node
Access Control	*MS/ Domain -specific*	Network layer access control using IP white/ blacklisting (Optional). Message processing (including receipt generation, payload delivery) restricted to authenticated parties subject to configured AS4 processing modes.	*MS/Non Domain -specific*	Each organization is individually responsible to implement security measures (e.g. ISO/IEC 27000) to protect access to its IT infrastructure, including its eDelivery infrastructure.

Authentication	*MS/ Domain -specific*	TLS server authentication (required); TLS client authentication (policy option for domains or parties). TLS version and cipher suites specification following ENISA guidelines. AS4 message layer authentication using XML Signature and WS-Security (required). Algorithms and key lengths following ENISA guidelines. Certificate requirements and distribution mechanism left to domains. Optional signing and validation of NAPTR records according to the procedures specified in DNSSEC. XML Signature applied to SMP XML response.	*MS/ Domain -specific*	(same as above applies)
Confidentiality	*MS/ Domain -specific*	TLS transport layer confidentiality. Version and cipher suites following ENISA guidelines. AS4 message layer confidentiality using XML Encryption and WS-Security (required). Algorithm and key lengths following ENISA guidelines. Certificate requirements and distribution mechanism left to domains.	*MS/ Domain -specific*	(same as above applies)
Integrity	*MS/ Domain -specific*	XML Signature and WS-Security applied to AS4 messages. XML Signature applied to SMP XML. Optional DNSSEC for BDXL records. (see Authentication).	*MS/ Domain -specific*	(same as above applies)
Non-repudiation	*MS/ Domain -specific*	Non-Repudiation of C2 as Origin using XML Signature and WS-Security (see Authentication). Non-Repudiation of Receipt by C3 using AS4 receipts, cryptographically tied to received message, signed using XML Signature and WS-Security (see Authentication above). Retention policies (logs, message stores, receipt stores) left to domains. XML Signature applied to SMP XML. Optional DNSSEC for BDXL records. (see Authentication).	*MS/ Domain -specific*	(same as above applies)
Accountability	n/a	n/a	n/a	(same as above applies)
Auditability	*MS/ Domain -specific*	n/a	*MS/ Domain -specific*	Both C2 and C3 must log all events that occur in the message exchange. It is up to the organization to ensure that the used SBB correctly implements the logging of events.

Table 14. Goal-based analysis of eDelivery

3.3.3. SAT Non-Repudiation

Non-repudiation services are mandated to generate, collect, maintain, make available, and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event, or action. Non-repudiation mechanisms provide protocols for the exchange of non-repudiation tokens specific for non-repudiation service. Such protocols may be classified upon the security property that they fulfil. Notably such properties as timeliness (awareness when the protocol ends) and fairness, have been considered crucial to the development of the e-SENS Non-Repudiation solution.

Many attacks can be performed on the non-repudiation services, e.g. to mask the occurrence of an event, forge the creation of an action, etc. Creating and providing a resilient non-repudiation protocol is a challenge the scientific community and the standardization bodies are faced by. Hence, re-using a well-known protocol has been considered crucial. For this reason, the e-SENS architecture provides an ISO/IEC 13888 compliant solution, which is flexible enough to cope with the various domain's needs.

The architecture is designed to emit any kind of evidence (with two capability realization with ETSI REM, and IHE ATNA) at any corner (with a proposed dispute resolution algorithm that embraces all the four corners) using any storage required by each backend regulation like, e.g., a revision safe archive (with a proposed realization using a request response protocol).

A high-level representation of the process is illustrated in **Figure 12**.

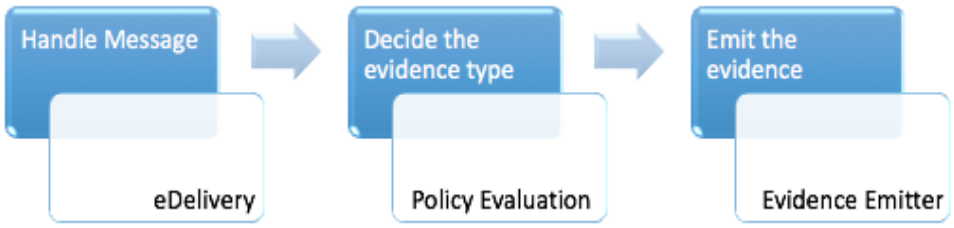

Figure 12. Non-repudiation in e-SENS

Non-repudiation mechanisms shall be regulated by policies and agreement. The Policy Evaluation component allows a XACML[19] representation of such agreements that can be linked by all the evidence generated, enabling a formal approach for the definition of dispute resolution algorithms. Policy evaluation further provides the Non-Repudiation ABB with flexible ways for configuration by editing the policies, the behavior, and the content of the evidence.

The content of the evidence is left unspecified, to cope with each domain's peculiarities albeit the e-SENS components propose two capabilities: ATNA and REM.

- ATNA is defined by the IHE ITI technical framework[20]. The content of each audit trail is classified by each application and project, and cannot be classified ex-ante;
- REM messages are of four kinds: non-repudiation of origin (NRO), non-repudiation of receipt (NRR), non-repudiation of submission (NRS), and non-repudiation of delivery (NRD). All these share the same syntax and semantics by ISO-13888 and thus they will be treated as generic "evidence tokens".

[19] eXtensible Access Control Markup Language, OASIS Standard: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[20] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf

Information	Sensitivity	Location	State	Security Goal
Evidence Token	non-confidential	Controlled (eDelivery Infrastructure)	Transmission, Storage	Non-Repudiation, Accountability, Auditability

Table 15. Information classification for Non-repudiation

The architectural decisions of the Non-repudiation SAT instruments the member states or the domain to define the content and the type of evidence to be emitted and stored. This analysis takes into account the Non-repudiation ABB realized as per-hop protocol.

Non-repudiation SAT	C1-C2	C2-C3	C3-C4	eDelivery Node (C2) or (C3)
Non-repudiation	Stores NRO for this corner and waits for the NRR generated by the next one and sent it back, for a particular message id	Stores NRO received by the remote corner, the NRR for this corner, generates a new NRO for the next corner and waits for the NRR generated by the remote corner	Stores NRO received by the remote corner, the NRR for this corner, generates a new NRO for the next corner and waits for the NRR generated by the remote corner	Stores and makes available the evidence
Accountability	as above	as above	as above	as above
Auditability	as above	as above	as above	as above

Table 16. Goal-based analysis for Non-Repudiation

It is worth noting that accountability may also need additional REM evidence type, related, e.g., to the event “login”. The evidence emitter enables auditability also in non-REM implementations (e.g., IHE ATNA).

3.3.4. SAT Trust Establishment

SAT Trust Establishment identifies technical means to establish trust in and between IT-Systems involved in cross-border / cross-solution electronic transactions through existing trust services. These “Trust Services” (TS) are electronic services which enhance trust and confidence in the electronic transactions provided by “Trust Service Providers” (TSPs)**.** Note that this SAT only references the means to be used by other SATs according to their security means and specific requirements regarding Trust Establishment.

Consumers and Providers of interconnected distributed solutions must be able to rely on and validate the authenticity and trustworthiness of each service/service-provider carrying out electronic transactions. This implies that mutual trust between services/nodes must be established.

In general, well-established security functionality according to mainstream international standards is referenced by this SAT, and most of the functionality is provided by runtime environments (operating systems, network technology).

On distributed electronic transaction/message level, cryptographic mechanisms are used for:

- authenticating entities involved in electronic transactions;
- authenticating claims presented by interacting entities, as may be required specific to underlying business scenario;

- authenticating requests to and outcomes of services, mostly by sealing/signing requests and responses/data delivered; electronic seals are applied to ensure integrity, too.
- securing data exchanged between entities (by means of signing and/or encryption).

These means are applied on network (using TLS) and/or message (using WS-Security) level using X509 certificates as security tokens.

Two main scopes must be distinguished regarding the technical means:

1) Iterative brokered trust and confidentiality, hop-to hop applied on network (using TLS) and/or message level (using WS-Security)
2) End-to-end trust in effect for Trust Establishment in business data (payload) exchanged; end-to-end encryption may be required in addition. Details of these means have to be agreed upon domain-wise on business application level.

In general, X509 certificates are used to apply electronic signatures / seals to ensure authenticity and integrity as well as encryption to ensure confidentiality. Different Trust Models per scope may be selected.

Trust must be established at least in the owner - Trust Service or users of such - of security tokens presented. This SAT addresses different models to establish trust, backbone of all of which is the conformance assessment and supervision of respective Trust Domain actors regarding the domain-wise defined policies and governance models.

Application domains may decide for one or a combination of Trust Models according their specific needs:

1) Direct Trust on base of controlled mutual key / trust-store exchange;
2) Dedicated trusted PKI based (actually in use: OpenPEPPOL PTN, CEF Digital Community PKI)
3) Trusted Lists based on ETSI TS 119 612 v2.1.1. These are the official MS Trust Lists at least for TS rated a qualified ones according eIDAS as well as domain TLs setup, e.g. for eTendering platform providers and their services.
4) extended Service Metadata Publisher (SMP) model, a specific eHealth profile to trustworthy expose certificates (in this 4-corner model case, certificates of C1/C4 in addition to respective C2/C3 ones), recently approved by OASIS as “Candidate Specification”.

Note: Different from 2), dedicated community PKI, the other options allow each entity for free choice of PKI/CAs of its choice respective possible national regulation in place for applicable PKI of public administration services.
Note that in a concrete domain scenario involving several hops in electronic transactions, the overall model could be Direct Brokered Trust, where nodes rely on each other in an iterative manner. This may be amended - like in the eJustice Domain - by providing a validation report (“Trust OK Token”) forwarded along with the transaction data.

Figure 13 gives an overview of Trust Models used, depicting the scope where they are applied for. As mentioned already, domains decided for different selection and combination of these models according to their needs.

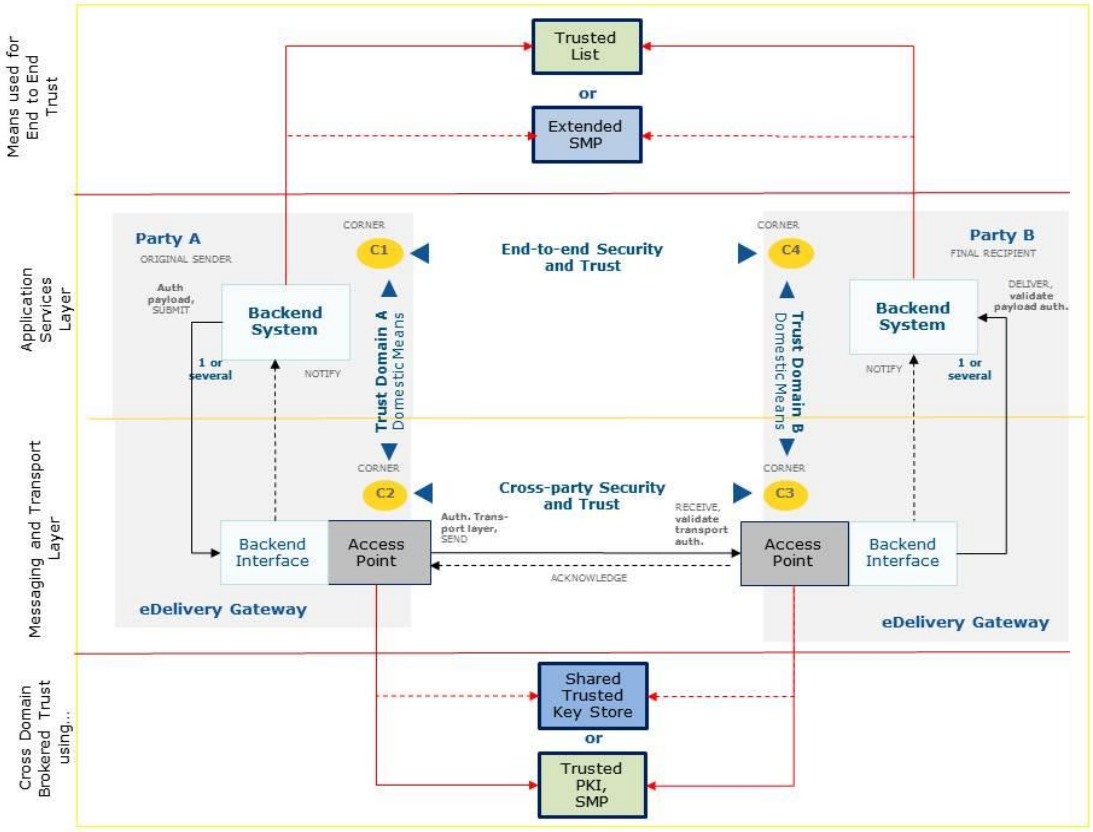

Figure 13. Trust Models as used in e-SENS - example for eDelivery

For brevity, the figure does not show the case of establishing trust in central or federated services consumed directly, bypassing the 4-corner eDelivery infrastructure. This applies for requesting e.g. SML/SMP services or national classification/code translation as used in eHealth. It's up to domains how to include such services in their Trust Model set up, principally all 4 options above would allow it. As the service type and trustworthiness of its provider probably are of high interest here, the TL or Trusted Key Store models have advantages, as so far SMP is focussed on the transport infrastructure components only - but the domain-based SMP extension model may be an option.

For this SAT, purpose of information is to validate a certificates / claims presented as - depending on the Trust Model in effect - being present in the respective Trust Domains repository or local Trust Store and valid at a certain time instant. Thus, this SAT deals just with lookup functionality.

Information	Sensitivity	Location	State	Security Goal
Security Token Lookup	Non-Confidential	Controlled (PKI-/ TL-/ SMP- Infrastructure; local Trust Store)	Transit	Integrity
Security Token Lookup Response	Non-Confidential	Controlled (PKI-/ TL-/ SMP- Infrastructure)	Transit	Authentication, Integrity

Table 17. Information Classification for Trust Establishment

Each organization is individually responsible to implement security measures to protect access to its IT infrastructure, this includes access to the eDelivery infrastructure (C1-C2 and C1-C4).

Means of Trust Establishment analysed here are not only relevant in context of the 4-corner model.

First of all, the trust models implemented in each of the domains have the eDelivery infrastructure as its underlying topology, but some domains in addition use central or federated services directly without involving eDelivery. Every active node involved in distributed electronic transactions must be able to validate authenticity and establish trust its source. The precise mechanisms, however, depend on the concrete domain or national setup. Therefore, the goal-based analysis performed for this SAT (and the resulting table) differs in its targets from the SATs previously described. In **Table 18**, Cx represents every active node in the infrastructure setup, including application services (C1/C4), eDelivery (C2/C3) as well as potential other services provided in a central or federated manner.

Trust Establishment SAT	Cx - Local Trust Store (lookup for trusted certificates)	Cx - Community PKI	Cx - Trust List	Cx - SMP
Access Control	n/a	n/a	n/a	n/a
Authentication	Authenticity of Trust Store and its updates provided centrally to be ensured	Authenticity given by trust in issuer certificates (Sub- and Root-CA)	Authenticity given by trust in Trust List operator certificate	Authenticity given by trust in SMP operator certificate
Confidentiality	n/a	n/a	n/a	n/a
Integrity	Integrity of Trust Store and its updates provided centrally to be ensured by validating its electronic seal when importing to local instance	Electronic seals are used to ensure integrity of OCSP / CRL responses, seal to be validated when processing OCSP/CRL responses.	Trust Lists SHALL be sealed by the Trust List operator, seal to be validated when consuming a TL.	SMP records are sealed by the SMP operator; in case of extended SMP used by eHealth the respective end-entity (in the 4-corner model in role C1/C4) initially seals its attributes to be published in addition. SMP operator has to validate the latter seal before publishing the SMP record, SMP record consumer has to validate the seal applied by the SMP operator.
Non-repudiation	n/a	n/a	n/a	n/a
Accountability	n/a	n/a	n/a	n/a
Auditability	n/a	n/a	n/a	n/a

Table 18. Goal-based analysis of Trust Establishment

It is assumed that mathematical validation of seals of messages/electronic transactions exchanged is done by the infrastructure components used (TLS and WS-Security implementation respectively). Only Trust Establishment in the certificates presented effectively differs per Trust Model.

Infrastructure and tools to maintain Trust Domain repositories are out of the scope of this SAT; mostly external services are used, like: RA/CA, registration at official MS Trust List, and SML/SMP registration. Maintenance and provision of domain Trust Stores and domain Trust Lists is operated on domain level. For the latter, the eTendering domain initiated the adoption and customization of the CEF Digital TL Manager Tool. This work, however, has to be accomplished by the OpenPEPPOL pre-award community.

For the models depicted above to establish direct C4 to C1 trust, a dedicated PKI may be an option,

too. A domain PKI in this case must cover registration of backend system instances, too, and issue certificates for those. This option was in discussion for the eTendering domain with OpenPEPPOL, but it has not been accepted so far. It may even be not acceptable in case national regulation is in place requiring from providers of public administration services to use dedicate national PKI. Finally, it is worth noting that for all Trust Models, the choice of a trust anchor is always a decision of the relying party.

3.3.5. SAT eDocument

An eDocument is an artefact that stores and route information in the context of an administrative process. An information security assessment of eDocument must take into account both the classification of the content and the interaction with other BBs that are used to create, store, transfer, access and protect the document itself. As an example, to ensure end-to-end security of eDocument during transport we can use eDelivery, while eSignature can be used to ensure integrity, even during the documents' storage. However, the Document Routing ABB in e-SENS leverages the use of metadata in a SBDH[21], which normally is unsigned, unencrypted and preserved during the end-to-end exchange of an e-document. The compromising of routing information may hinder eDelivery effectiveness and the desirable end-to-end document integrity (from Originator to Receiver); therefore, to guarantee the integrity of SBDH during all exchanges in the 4-corner model one must rely on underlying transport protocols (besides the cross-border exchange). Non-Repudiation SAT can also provide integrity and authentication mechanisms to Document Routing ABB when applied to all transmission exchanges.

This section deals mainly with business documents, since the security analysis of messages can be derived from the information contained in the section of the BBs that exchange the messages themselves. However, there is no conceptual difference between messages and documents and the approaches adopted to secure the former can also be adopted for the latter. Furthermore, we must consider that when a Container[22] is used to wrap up and route a group of documents, the container itself is a document as well.

A high-level representation of the document usage in a 4 corner model is illustrated in **Figure 14**, where C1 is the eDocument producer, C2 is the producer's gateway, C4 is the eDocument Consumer and C3 is the Consumer's gateway. The signing-encryption and validation pipeline is evident.

[21] UN/CEFACT Standard Business Document Header

[22] Ref to ETSI ASiC spec: 3.1 Definitions: file holding data objects with related manifest, metadata and associated signature(s), under a specified hierarchy comprised of a data object (any digital information to which Advanced Electronic Signature(s) and/or time-stamping are applicable) and metadata (data describing context, content and structure of data objects and their management over time).

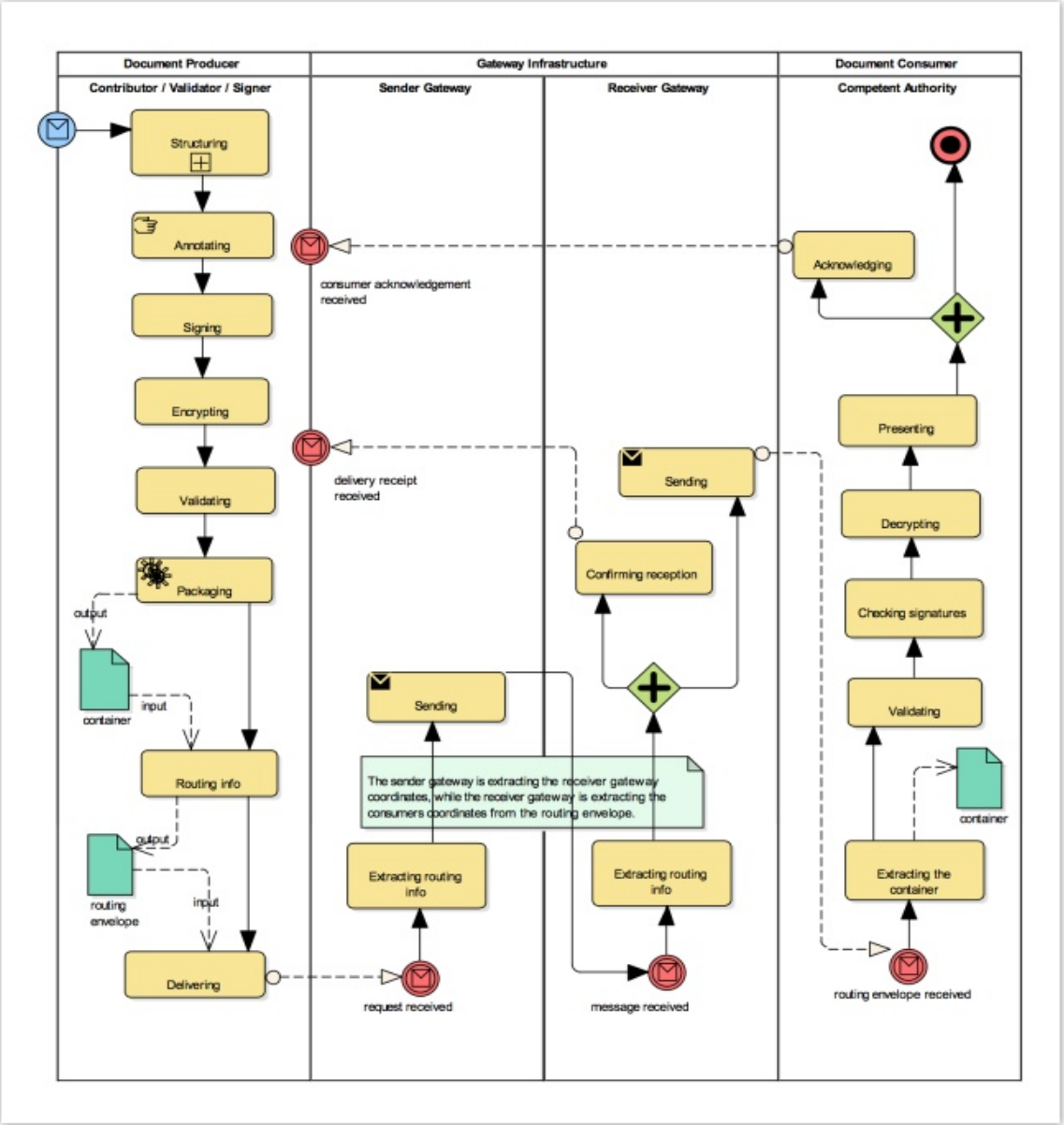

Figure 14. eDocument Architecture

The usage of a container can address many security goals, since it can guarantee the confidentiality and integrity of the documents contained, their authenticity and non-repudiation (both the container and the content can be signed), and in some cases even used for access control purposes. ENISA offers guidelines on the algorithms and key lengths that must be adopted to enforce security measures on eDocuments[23]. Confidentiality can be ensured using encryption or enclosing the content in a folder (a "container") and leveraging access policies.

[23] The EC Regulation 611/2013 (link below) references ENISA as a consultative body, in the process of establishing a list of appropriate cryptographic protective measures for personal data protection, which are made available in the form of guidelines: and studies on cryptographic protocols.
(see e.g. .Algorithms, key size and parameters report 2014:
https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014)

When used to represent business information, an eDocument may contain legal, personal or business-critical information; therefore, security requirements must be specified considering Data Protection Regulation (GDPR)[24] and the risks associated with exposing the exchanged information.
Most countermeasures adopted for eDocument rely on encryption, electronic seals[25], and eSignatures applied during the eDocument creation phase or during routing. These tools are used to preserve confidentiality, integrity, non-repudiation and auditability of the documents, while confidentiality of sensitive information can be guaranteed through access control mechanisms.

Information	Sensitivity	Location	State	Security Goal
Messages	Sensitivity depends on the content - metadata usually do not contain sensitive data, while payload can contain business information and personal data.	transmission infrastructure, data stores, processing units	Creation, Transmission, Storage, Processing	Integrity, Non-repudiation, Accountability, Auditability, Confidentiality (depending on the content)
Business Documents	Business documents usually contain sensitive information and personal data.	transmission infrastructure, data stores, processing units	Creation, Transmission, Storage, Processing	Confidentiality (depending on the content), Integrity Non-repudiation, Accountability, Auditability

Table 19. Information classification for eDocument

eDocuments SAT	C1-C2 C3-C4	C2-C3	End-to-End	as a Document
Access control	Needs adequate organizational and technical policies. Can use eID. Container can provide further layers of access control[26]	Needs Message Exchange ABB Container can provide further layers of access control	Provided by Trust ABB (Encrypted with recipient's encryption key)	encryption / container
Authentication[27]	Needs eSignatures + Trust ABB Routing[28]: needs adequate transport protocol (not specified) or organizational policies, or Non-	Needs eSignature + Trust ABB Routing: provided by Message Exchange ABB	Needs eSignatures + Trust ABB Routing: needs Non-repudiation ABB	eSignatures

[24] 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, repealing Directive 95/46/EC (General Data Protection Regulation) ; 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, repealing Council Framework Decision 2008/977/JHA.

[25] eIDAS: (59) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.

[26] As per Document Packaging ABB of eDocument SAT.

[27] Authenticity is the security goal for eDocument as an artifact; Authentication is left here for coherence, and it is intended as the security goal for eDocument as a service.

[28] As per Document Routing ABB of eDocument SAT.

	repudiation ABB			
Confidentiality	Container w/ encryption Routing: n/a	Container w/ encryption Routing: n/a	Container w/ encryption Routing:n/a	encryption
Integrity	Container w/ signature Routing: needs adequate transport protocol (not specified) or Non-repudiation ABB	Container w/ signature Routing: needs Message Exchange ABB or Non-repudiation ABB	Container w/ signature Routing: needs Non-repudiation ABB	eSignatures (signed digests)
Non-repudiation	Container w/ signature Routing: needs adequate transport protocol (not specified) or Non-repudiation ABB + Trust ABB	Container w/ signature Routing: needs Message Exchange ABB or Non-repudiation ABB, plus Trust ABB. Retention policies depend on the content. Logs must not contain personal data. No documents should be stored while on transit if they contain personal data (GDPR is to be taken into account).	Container w/ signature Routing: needs Non-repudiation ABB + Trust ABB	eSignatures, Seals
Accountability	eSignatures and Digests required	End-to-end Authenticity is managed through eSignature or container signing. Signed and encrypted digests can provide evidence of routed eDocuments on the gateway level, as logs should not contain personal data.	eSignatures, Digests	eSignatures, Digests
Auditability	Container w/ signature and Timestamp UUID[29] from eDocument Provisioning or Routing ABB's.. Non-repudiation ABB w/ Per-Hop Protocol	Needs Non-repudiation ABB w/ Per-Hop Protocol or Message Exchange ABB	Needs Non-repudiation ABB w/ Per-Hop Protocol + correlatable evidence per exchange, e.g. a UUID from eDocument Provisioning or Routing ABBs	eSignatures, Digests

Table 20. Goal-based analysis for eDocument

3.3.6. SAT Semantics

Out of the four BBs comprising the SAT Semantics, the domain specific and the core vocabularies are publicly shared and abstract non-confidential information. Therefore, the main security goals for core and domain specific vocabularies are integrity and availability. On the other hand, semantic mappings and Base Registries are trusted sources of information that can potentially give access to confidential or sensitive data. These sources of information can be accessed through eDelivery network or as REST[30] web Services, using an URL to access the state of the semantic resources.

Well known examples of Semantic Mapping services are the DNS system, specifies a mapping between

[29] ITU-T Rec. X.667 | ISO/IEC 9834-8 Universally Unique Identifier

[30] REST (REpresentational State Transfer) is the architectural style of the World Wide Web, defined by Roy Fielding. In the REST architecture style, clients and servers exchange representations of resources by using a standardized interface and protocol. Resources are decoupled from their representation so that their content can be accessed in a variety of formats. Metadata describe the resources and are used to control caching, detect transmission errors, negotiate the appropriate representation format, and perform authentication or access control.

URLs [RFC2915, RFC4848] and the location of resources in an infrastructure [RFC3401, 3402, 3403, 3404] and the SMP, that maps Participant Identifier on information on the document types can be handled by a specific Participant Identifier.

From an architectural point of view, the entire spectrum of security goals applies to these two BBs, but a preliminary risk analysis should be performed to select the adequate measures to be applied in the specific cases and consequently the solutions that fit the needs.

In the following, the security measures will be tailored on the architectural style of interaction, depending on whether a REST interaction is selected or e-Delivery.

At the transport level, a Mapping Service and Base Registry access may either be secured or unsecured depending on the specific requirements and policies adopted by the business document exchange infrastructure and the sensitivity of the information exchanged. Likewise, client-side authentication MAY be supported by these services pending infrastructure requirements and policies.

Semantics SAT	Sensitivity	Location	State	Security Goal
Domain Specific Vocabularies, Codelists	non-confidential	public (in base registries); Controlled[31]	Transmission, Storage, Processing	Availability, Integrity, Auditability, Non-Repudiation, Accountability,
Core Vocabularies	non-confidential	Public for requests[32]; Controlled (same as above)	Transmission, Storage, Processing	Availability, Integrity Auditability, Non-repudiation, Accountability,
SemanticMappingRequest	non confidential or confidential [33]	Controlled - the solutions depend on the interaction style (eDelivery or REST)	Transmission, Storage, Processing	Access Control, Availability, Integrity, Non-Repudiation, Accountability, Auditability
SemanticMappingResponse	in most cases confidential (mediates the access to business information)	Controlled (under the management of an organization or community)	Transmission, Processing	Access Control, Availability, Integrity, Non-Repudiation, Accountability, Auditability
BaseRegisterAccess Request	non confidential or confidential, (same as above applies)	Controlled (same as above)	Storage, Transmission Processing	Access Control, Availability, Integrity, Non-Repudiation, Accountability, Auditability
BaseRegisterAccess Response	confidential	Controlled (same as above)	Transmission, Processing	Access Control, Availability, Integrity, Non-Repudiation, Accountability, Auditability

Table 21. Information classification for Semantics

For the Semantic Mappings Services and the Base Registries, the managing organization is responsible for ensuring availability, accountability and auditability of the service (logs, message stores, receipt stores); technical solutions are available to ensure Non-Repudiation of the service as Origin of the mapping (e.g. using XML Signature and WS-Security). Additional measures to insure confidentiality during transport are to be undertaken in the case the service gives access to personal or confidential

[31] Releases updates and change requests (a consensus-making and management process) must be in place

[32] In base registries or in repositories, like Joinup: https://joinup.ec.europa.eu/asset/core_vocabularies/description

[33] Depends on the data sources accessible through the service

data.

In case the base register contains personal or sensitive data, there can be constraints on where data is located (see Data Protection regulation)[34]: eIDAS and eDelivery infrastructure can be combined with a Base Registry in order to guarantee authentication of the accessor and confidentiality during transmission of the data that is being accessed and transferred to the data consumer.

Semantics SAT[35]	eDelivery Interaction[36]	REST interaction
Access control	Signature or seals on the requests and responses. The signer certificates are published in Metadata files that must be signed by MS-notified certificates. Each organization is responsible to protect the access to its eDelivery network.	SSL access to API URLs; Role Based access control on the server side. The same techniques used for DNSsec can be applied to secure access to Semantic Mapping Services. [RFC 2535; RFC 4035; RFC 4509] Access Policies can be encoded in XACML[37]
Authentication	TLS server authentication (required); TLS client authentication (policy option for domains or parties). TLS version and cipher suites specification following ENISA guidelines. AS4 message layer authentication using XML Signature and WS-Security (required). Algorithms and key lengths following ENISA guidelines. Certificate requirements and distribution mechanism left to domains.	eSignature and validation of NAPTR[38] records according to the procedures specified in DNSSEC. XML Signature applied to XML response if accessed by REST, like in SMP
Confidentiality	e-Delivery TLS transport layer confidentiality. Version and cipher suites following ENISA guidelines. AS4 message layer confidentiality using XML Encryption and WS-Security (required). Algorithm and key lengths following ENISA guidelines. Certificate requirements and distribution mechanism left to domains.	In the case the service gives access to confidential or personal data, confidentiality has to be met by encryption of the payload and access control - note that usually REST does not provide confidentiality of data; since responses are authenticated but not encrypted.
Integrity	XML Signature and WS-Security applied to AS4 messages. XML Signature applied to SMP XML. Optional DNSSEC for BDXL records. (see Authentication).	Integrity of data in transit provided by TLS. Public key encryption guarantees confidentiality but not integrity since the receiver's public key is public. For the same reason, encryption does not ensure the identity of the sender. XML signatures provide message integrity using the sender's private key. This signature can be validated by the recipient using the sender's digital certificate (public key).

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

[35] Only referred to Base Registries and to Semantic Mapping Service when it grants access to sensitive data, e.g. to evidence in the future e-CERTIS evolutions

[36] The description here is focused on the cross-domain (C2-C3) interaction, since in the intradomain, each organization is responsible to protect the access to e-Delivery network and then to secure the interaction at C1 - C2 and C3-C4.

[37] XACML defines a core XML schema for representing authorization and entitlement policies.

[38] Name Authority Pointer (NAPTR) is a type of resource record in the Domain Name System of the Internet. NAPTR records map between URNs, URLs and domain names [RFC2915].

Non-repudiation	Non-Repudiation of C2 as Origin using XML Signature and WS-Security (see Authentication). Non-Repudiation of Receipt by C3 using AS4 receipts, cryptographically tied to received message, signed using XML Signature and WS-Security (see Authentication above). Retention policies (logs, message stores, receipt stores) left to domains. XML Signature applied to SMP XML. Optional DNSSEC for BDXL records. (see Authentication).	Part of the techniques used in the case of eDelivery can be used. Usually Non-repudiation relays on the presence of Trusted Third Parties and the use of eSignature and Timestamps. Retention policies (logs, message stores, receipt stores) left to domains. XML Signature applied to XML payload. Optional DNSSEC for BDXL records. (see Authentication).
Accountability	End-to-end Authenticity is managed through eSignatures. Signed and encrypted digests can provide evidence of routed response Messages on the gateway level, as logs should not contain personal data.	End-to-end Authenticity is managed through eSignatures. Signed and encrypted digests can provide evidence of routed response Messages on the gateway level, as logs should not contain personal data.
Auditability	Managed through eSignatures, Timestamps and the use of Trusted Third Parties. The managing organization is responsible for ensuring the auditability of the service (logs, message stores, receipt stores)	Managed through eSignatures, Timestamps and the use of Trusted Third Parties. The managing organization is responsible for ensuring the auditability of the service (logs, message stores, receipt stores)

Table 22. Goal-based analysis for Semantics

3.3.7. Summary of EIRA Security Analysis

The SATs (together with all their ABBs) analysed here were: eID, eDelivery, Non-Repudiation, Trust Establishment, eDocuments and Semantics. With this, all of the EIRA artifacts were embraced by the security analysis.

This analysis of the EIRA demonstrate that the specifications are grounded on well-established security standards and solutions. Furthermore, all of the security goals can be addressed by adopting some (or a combination) of the EIRA's building blocks (BBs). Information in all its states and locations can be adequately accounted for, depending on its sensitivity, in order to address a certain security goal.

One of the most important traits of the EIRA is that its building blocks are fully interoperable in various combinations that may require their interdependence. Although this remark is not relevant only from a security aspect, in this particular context it also becomes evident that by interconnecting the relevant BBs, a certain security property can be leveraged to meet any of the security goals/objectives.

By presenting a high-level overview of the architecture to which each of the security mechanisms apply, and by providing a catalogue of the security goals addressed by each of the SATs, a non-technical person is able to grasp the capability of a certain e-SENS solution that is aimed to satisfy a certain security requirement. Moreover, by providing a detailed elaboration of the technical processes that stand behind a certain solution and an adequate reference to the standards on which it is based, a technical person can get the support needed to build a conceptual model of a solution aimed at satisfying a particular security requirement. Hence, the analysis performed here also provides a common ground for understanding between various layers of experts in a given organization.

At this point, the rationale behind associating e-SENS with a "Lego-brick metaphor" also becomes evident: even the security solutions enable new domains in using a set of the EIRA building blocks adjusted to a specific business need. However, the fact that EIRA operates on architectural level and that the building blocks serve various purposes and apply different standards and security solutions call for additional analysis. On the one hand, such analysis would serve as a proof-of-concept on what has been presented in this section. On the other hand, it would provide additional insights into the

behaviour of the building blocks in an operational setting. Therefore, security analysis of practically implemented solutions is also performed and presented in the next section.

3.4. Security analysis of the pilots

In order to provide a holistic view of the security evaluation of the e-SENS building blocks, a Questionnaire (see Annex IV) was designed with the aim to extract experts' insights and experience regarding the implementation of trust and security mechanisms within the pilots. In addition to the security aspects, more general systemic properties are also addressed by the questionnaire contents. The results from the processed responses aim to directly answer to the objectives of the deliverable, but at the same time provide a view on the dependencies and interrelations between the BBs' specifications and their actual implementations.

Security questionnaire design

The questionnaire is designed according to the RMIAS (Reference Model for Information Assurance and Security), which is the same reference model employed in the cybersecurity evaluation of the EIRA. The reference model guides both the nature of the questions and the structure of the questionnaire itself.

The Questionnaire is divided into five sections, four of which integrate the separate dimensions of the RMIAS (Security goals, Countermeasures, Information Taxonomy and System Security Lifecycle), and one section devoted to Trust models implemented by the pilots. The System Security Lifecycle is to a great extent an assessment of the general systemic properties of the security mechanisms and helps to get insights into the sustainability of the security solutions.

3.4.1. Results and analysis

The questionnaire was sent to the relevant experts of all piloting domains. As some of the domains employed identical mechanisms, a joint response was provided in those cases. For example: eAgriculture, Nemkonto, eEducation, Record Matching were all addressed by a single feedback for the Citizen Lifecycle Patient Access pilot. In the same way, Business Registration and Activity Registration are both contained in the response provided by the Business Lifecycle pilot.

The respondents to the questionnaire include almost all of the domains integrating an e-SENS solution, except eJustice. From eProcurement, feedback was delivered for eTendering, eInvoicing and VCD, from eHealth: for ePrescription/Patient Summary and eConfirmation; from Citizen Lifecycle: for eAgriculture, Nemkonto, Patient Access, eEducation, and Record Matching; and from Business Lifecycle, for Business Registration and Activity Registration.

Following are the comparative and qualitative analysis of the provided feedback, divided according to the questionnaire sections, i.e. the reference model dimensions.

Security goals

The first section of the Questionnaire investigated the employment of security mechanisms to address the security goals set by the project. As shown in **Figure 15**, all security goals set to be addressed by the specifications have been a requirement that was also addressed by one or more of the pilots.

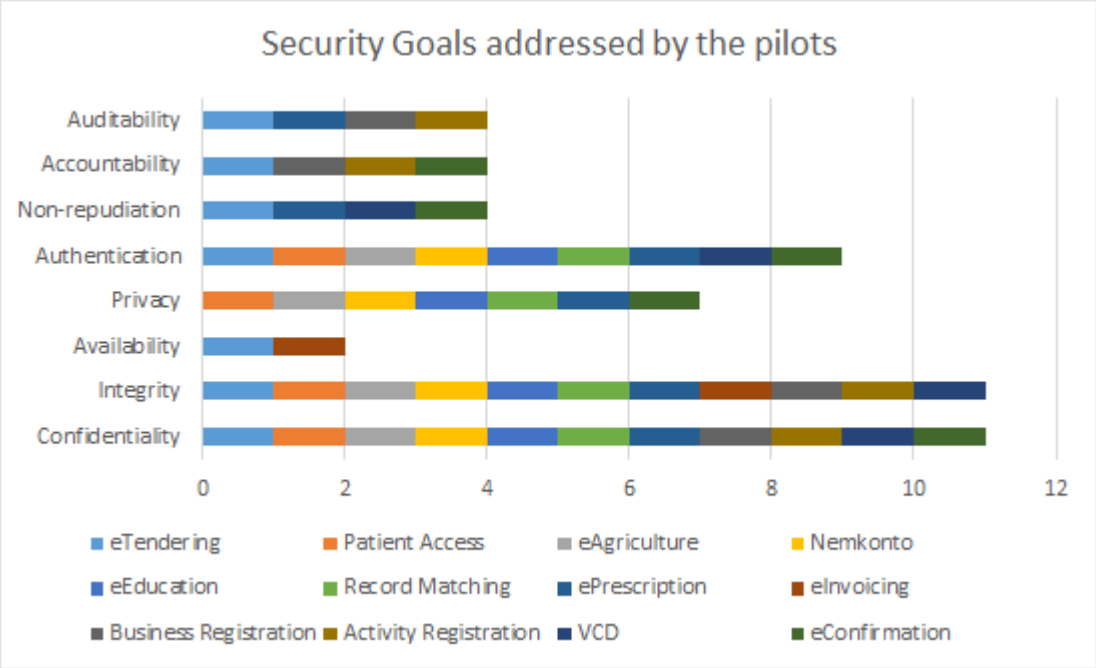

Figure 15. Security goals addressed by the pilots

The eTendering pilot employed mechanisms for addressing almost all of the security goals, which is to some extent expected, considering the fact that information was tackled in all the states during its lifecycle, and all of the assets' security has to be addressed (as discussed in the next section).

Confidentiality and Integrity were addressed by almost all of the pilots, whereas the results for Availability point to a high probability that further considerations are needed in that direction.

One may certainly deliberate along the following lines: assuring availability of all resources and hardware, fault-tolerance and redundancy is mainly Member State dependent, and Member States are expected to comply with Article 13a[39]. However, considering the fact that Hardware, Software and Networks are among the security assets stated by the pilots, Availability is expected to be among the top security goals to be addressed. The fact that no pilot has reported consideration of Redundancy and Fault-tolerance, thus, comes as no surprise. At the same time, it reveals a need for better consideration and proper accounting for Availability as one of the major security goals.

Information taxonomy

Information in e-SENS has been tackled in all the phases of its lifecycle: Creation, Transmission, Storage, Processing, and Destruction (**Figure 16**).

[39] Paragraphs 1 and 2 of Article 13a:

"1. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organizational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimize the impact of security incidents on users and interconnected networks.

2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks. […]"

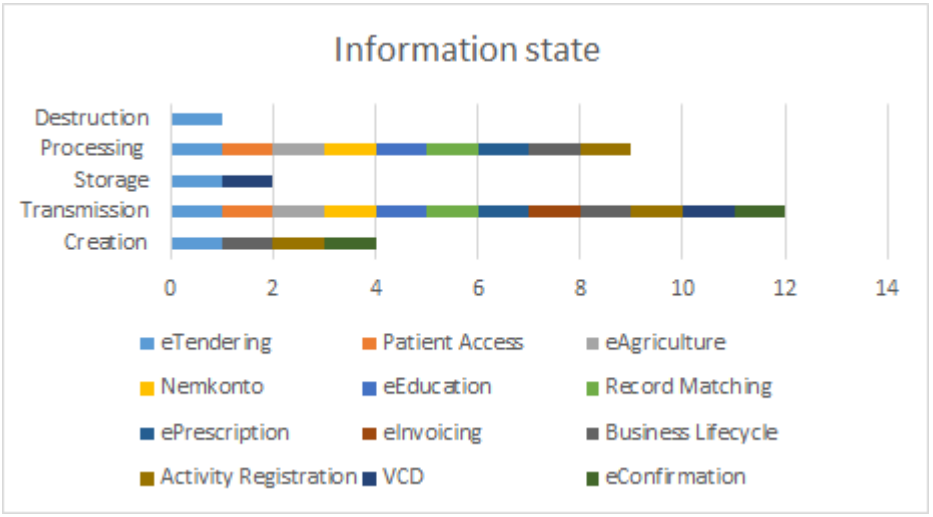

Figure 16. The state in which Information is being dealt with by the pilots' security mechanisms

Not each pilot has employed mechanisms to handle information securely in each state, but all pilots ensure secure transmission of information. However, dealing with information in a particular state is highly context-dependent, so no claim can be made of whether there is a lack of certain security mechanisms or if information is not handled in a secure manner in some state. Secure processing and creation of information is also addressed to a great extent.

Variety of entities were concerned by the implementation of the security mechanisms, among which Information is the main asset that is being tackled (as shown in **Figure 17**). Software, Networks, Processes and People are also major security assets, whereas Hardware is being tackled to the least extent.

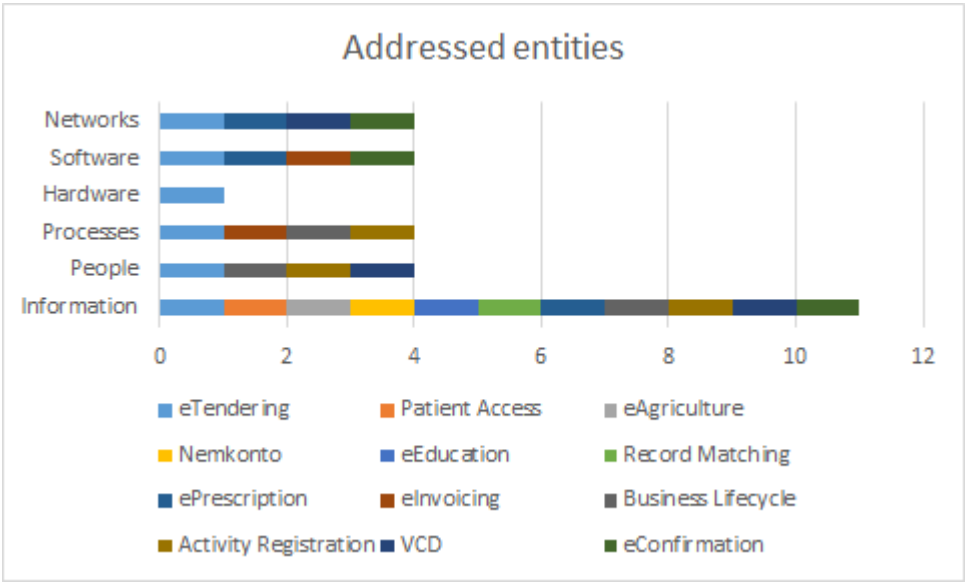

Figure 17. Entities concerned with the implementation of the security mechanisms in the pilots

But it is not only the number of the security assets and the frequency of implementation of a certain security mechanism that counts; the impact of the particular asset for the overall system and the impact of the failure of a certain security mechanism are also very important. The choice of entities that would be addressed by the security goals is clearly both context- and mechanism -dependent.

However, as humans are the core of the system, it can be observed that not all pilots considered the human-factor as part of the overall system security. This is especially important if one takes into account that countermeasures can come in legal, organizational and strictly human-oriented manner. The next section presents more detailed analysis in this direction.

Countermeasures

Regardless of whether a certain pilot implemented its security mechanisms with a concrete threat-model in mind, countermeasures could still be in place due to mere operational system requirements. The following countermeasure were investigated by the questionnaire: i) technical; ii) legal; iii) organizational; and iv) human-oriented.

Technical countermeasures that are widely employed by the pilots are encryption and authentication. This is conveniently complemented with legal countermeasure in the form of agreements/contracts, whose type (community, multilateral, etc.) depends on the needs of the pilot. When employed, policies are the usual choice for an organizational countermeasure. Audit was reported by only one of the pilots (eConfirmation). Human-oriented countermeasures are largely lacking, with 'Motivation' and 'Operational guidelines' being the only approaches taken. However, this is to a certain extent expected, as this would mainly be a Member State-specific requirement, which is out of the scope of e-SENS pilots.

The implementation of countermeasures is, as well, domain-dependent. Not every pilot has the same assets to secure or deals with the same extent and nature of risks. For example, whereas most of the pilots employ only encryption and authentication as technical countermeasures, the eHealth pilot also has policy-based access control for authorization in place (XACML), and patient informed consent (BPCC) to address Privacy.

Finally, monthly cross-border interoperability tests (known as connectathons) have been carried out by the pilots, but no special attack or breach-driven test have been done so far by any of the pilots.

Trust

The employment of trust mechanisms contributes for enhancing Integrity and Accountability security goals. Confidentiality, although mainly addressed by means of encryption, is also strengthened by the notion of trust in the underlying infrastructure. The purpose and the reasons of implementing one trust model over another is not in the scope of this analysis and is described in more details in the security analysis of the Trust Establishment SAT in Section 3.3.4.

All pilots employ one or more types of trust mechanisms, depending on the needs of the intradomain or the cross-domain trust establishment. The Trust Network PKI ABB is the most widely employed building block from the Trust Establishment SAT. Nevertheless, all of the Trust Establishment ABBs find their usage in some of the pilots, or an aspect of the pilot implementation thereof.

One issue that was reported through the pilots' feedback is that self-signed certificates are still widely used. Under certain conditions (e.g. if the parties know and trust each other to protect their own respective private key, and if they can confirm the accurate transfer of public keys), self-signed certificates may decrease the overall security risk of a transaction. However, they cannot be revoked, which may allow an attacker with authorized access to monitor and inject data into a connection or to spoof an identity if a private key has been compromised. This also points to the need of performing adequate risk analysis that is domain-dependent, something that has not yet been done in any of the pilots.

Security system lifecycle

This section of the questionnaire aimed at exploring the general lines of development of the security mechanism itself. In a sense, it extracts a bigger picture of the security design and management of the system in order for a system designer to grasp the high-level problems that might appear in the development lifecycle.

In that context, most of the pilots base the choice for employing trust and security mechanisms on an inherited infrastructure (from previous projects). The results are to a certain extent a testimony of the ability to adapt the latest security mechanisms to earlier security infrastructures. More importantly, this adaptability of the security solutions is an additional argument for the EIRA's sustainability with respect to the security capabilities provided by its building blocks. Therefore, the fact that all the pilots claim low expectation for frequent mechanisms' updates comes as no surprise. A note on the relative stability of the security mechanisms can be made coming from the mere fact that all of the security experts responded that small changes in the security mechanisms would not have big impact on the remainder of the system.

However, there is a need for redundancy considerations, as most of the pilots reported of no redundancy considerations in the security mechanisms' design. In the same sense, risk-assessment has not been done for any of the pilots. Although in one of the feedbacks it was reported that the security mechanisms for the pilot were chosen with a particular threat model in mind, no additional information or evidence about performed risk analysis or any kind of security risk management has been provided.

Discussion

While not all of the pilots address all of the security goals or employ counter-measures for all the threats possible, the fact that all of the security goals were addressed, information has been accounted for in all of its states, all of the entities in question were tackled by some of the security mechanisms and countermeasures are in place from technical, legal, human and organizational aspect, speaks of the fact that the EIRA is able to answer to all of the current cybersecurity requirements set by the pilots. The mere ability to provide a feedback loop to the cybersecurity evaluation of EIRA demonstrates its flexible nature and the readiness to respond to architectural needs, in the sense that it is lendable to both empirical and theoretical evaluation.

It is important to note that, in addition to information about the security mechanisms employed by each of the pilots, the analysis of Information Taxonomy (followed by a graphical representation of the results) provides insights into the security goals that each of the pilots is expected to meet, depending on the information state and the entities that are being tackled.

Certainly, the mechanisms employed largely depend on the particular context and use case and cannot be joined by a single universal security mechanism. That is only an argument for the strength of the e-SENS building blocks: they are generic enough to embrace various domains, yet specific enough to adapt to the domain's needs. In that regard, the results from the questionnaire demonstrate that the generic security properties provided by the EIRA are also resembled by the pilots. The domain-specific properties can also be seen in the results, and they can be further mapped onto the EIRA and translated into generic ones at a later stage, if shown to be evolutionary 'ripe' for becoming systemic security properties.

A more detailed security discussion will be provided after complementing the goal-based approach with a threat-view on the e-SENS security management.

3.5. Threat-based view in the cybersecurity analysis (EIRA and pilots)

The implementation of cross-border eServices, and the shift towards a more open government/public administration have created many opportunities for electronic experiences that are not only expected to be interoperable, but also cross-contextual. At the same time, such openness created a fertile soil for new vulnerabilities and opportunities for the cyber-attackers to exploit them.

In terms of means employed in response to the attacks, cyber defence varies to a great extent and there is a need for a clear recommendation framework to align the cybersecurity strategies and requirements across administrations and sectors. Risk assessment and management frameworks providing guidelines for securing and continuously improving information systems do exist and are usually complemented with the enforcement of adequate information security policies by means of rights and obligations, incentives and sanctions.

As stated in the preceding section, the cybersecurity analysis presented in this deliverable is mainly goal-based, as threat- or risk-based approaches are usually in need of statistics of former system behaviour or other data to thoroughly evaluate risks and vulnerabilities of a system. Furthermore, a threat- or risk-based analysis is only as complete as the experience of the analyst allows it. However, EIRA is not just a concept, and results from e-SENS have reached sufficient technical maturity. Therefore, it is necessary not only to regard the process leading to a solution, but also the solution itself and include all actors involved in the process. In that sense, a threat-view on the security management in e-SENS (not a threat-modelling process for each of the solutions) is necessary in order to complement the previous cybersecurity analysis.

In the following subsections, a more detailed elaboration is given on where and how threat-analysis is applicable to e-SENS for security purposes. Some related projects and initiatives are outlined first, together with relevant assessment frameworks for threat-based security management. A methodology for extraction of operational recommendations for security measures in e-SENS is then presented. Based on the outcomes of the methodology, the sophistication level of the security measures in e-SENS is then assessed. In the end, a discussion is provided on the cybersecurity analysis presented in this deliverable.

3.5.1. Related initiatives and regulatory frameworks

EU is making significant steps toward cross-border eServices implementation and the interoperability of such solutions. Improvements are being made in regulating and protecting the sectors that involve dealing with sensitive data and critical infrastructures' maintenance. In this regard, dedicated measures and efforts are being taken to include additional domains on the list of critical infrastructures. To provide a strategy of cyber defence is becoming a priority across all the Member States. For example, in the 2017 edition of eGovernment factsheets, which summarise policies and activities related to the implementation and the delivery of digital public services in 34 countries, cybersecurity is enlisted as an emerging topic. The advances in digitalisation of public services is recognized to come with an increase of risks of security breaches. Consequently, many cybersecurity strategies were launched throughout the continent. For example, Malta adopted a National Strategy on Cybersecurity in the second half of 2016, Slovakia adopted an Action Plan for the Implementation of the Cyber Security Concept in March 2016, and the UK has launched its National Cybersecurity strategy in November 2016.

The NIS Directive aims at ensuring a high common level of network and information security ("NIS") across the EU. Being the main piece of legislation of the "2013 EU Cybersecurity Strategy", it requires operators of critical infrastructures and digital service providers to adopt appropriate steps to manage security risks and to report serious incidents to the national competent authorities. Energy, transport,

banking, financial market infrastructure (trading venues, central counterparties), health, water, and digital infrastructure (internet exchange points, domain name system service providers, top level domain name registries) are some of the sectors of the economy that are impacted by the NIS Directive. Moreover, the digital service providers are also subject to compliance with the NIS Directive: online marketplace, cloud computing services.

Being part of the Framework Directive 2009/1401/EC within the Telecom Package, the set of obligations in Article 13a aims at ensuring the security and integrity of electronic communication networks and services, dealing mostly with availability of services. As a response to the directive's requirements, ENISA, Ministries and NRAs from member states, have initiated a series of meetings in order to achieve a harmonized implementation of Art. 13a. Three non-binding technical documents were provided as guidance to the NRAs in the EU member states: Technical Guideline on Incident Reporting, Technical Guideline on Security Measures and Technical Guideline on Threats and Assets.

The ENISA technical guideline on security measures sublimes an extensive list of national and international EU electronic communications standards into a set of security objectives divided by domain. It outlines 25 security objectives, each of which is further analysed through various security measures and supported by a set of evidence that serve to justify a statement that some objective was met. The security measures are grouped in 3 sophistication levels, whereas the security objectives are divided in 7 domains of application. This leads to an approach that is general enough to be understood by all the relevant experts and the management team in an organization, and specific enough to deliver the threat analysis necessary to complement a goal-based approach. For these reasons, the ENISA guidelines are chosen as a suitable framework in providing complementary views to the goal-based security evaluation based on RMIAS[40]. As such, the guidelines are analysed in more detail according to the cybersecurity evaluation needs. The Methodology of the approach is presented here, whereas the threat-view and the analysis themselves are part of Annex I and Annex II, in order to keep the clarity of the text here.

Providing a catalogue of all the security measures that a certain objective may include is out of the scope of the current evaluation. They can be found in the ENISA technical guidelines on security measures.

3.5.2. Methodology

There is criticism about frameworks deemed to be too focused on the technical aspects of design and falling short in addressing and detecting potential design conflicts (c.f. Uncommon criteria). An example of a problem arising from this point would be a system that is supposed to implement both anonymity and auditability. Therefore, a more general framework may be needed that would be both understandable enough by the non-technical person, but that still offers sufficient technical guidelines that are expected from a threat-based approach. Based on the previous elaboration on the ENISA technical guidelines for security measures, and after careful consideration by the WP6 experts through constructive debates during face-to-face and remote meetings, it was agreed that an effort to provide a complementary threat-view of the goals-based analysis may be beneficial for extracting operational recommendations on the security issues in e-SENS. This possibility was further evaluated by mapping the objectives of the ENISA guidelines onto the e-SENS security goals. The evaluation is presented in Annex I, together with the comparative analysis of the ENISA guidelines vs. the goal-based approach of RMIAS.

The e-SENS security measures have been assigned a sophistication level according to the **ENISA**

[40] Reference Model for Information Assurance and Security

guidelines. e-SENS security measures (aimed at meeting security objectives set in ENISA guidelines) are grouped in three sophistication levels as shown in **Table 23**.

Each level of sophistication corresponds to some criteria to judge whether it is attained; the results are backed with the evidence gathered in support of the judgement.

The reported results are based on the outcomes of the BBs and Pilots security evaluation and they are assigned according to the methodology adopted (ENISA guidelines).

ENISA description of sophistication levels	Assessment of the e-SENS security measures	
	LEVEL ATTAINED?	EVIDENCE
Level 1 (basic): - Basic security measures that could be implemented to reach the security objective. - Evidence that basic measures are in place.	**Yes**	Basic security measures are in place - see BB's security evaluation and the pilots security evaluation
Level 2 (industry standard): - Industry standard security measures to reach the objective and an ad-hoc review of the implementation, following changes or incidents. - Evidence of industry standard measures and evidence of reviews of the implementation following changes or incidents.	**Yes**	Industry security measures are in place - see pilots security evaluation and the assessment of technical maturity of the EIRA's building blocks
Level 3 (state of the art): - State of the art (advanced) security measures, and continuous monitoring of implementation, structural review of implementation, taking into account changes, incidents, tests and exercises, to proactively improve the implementation of security measures. - Evidence of state of the art (advanced) implementation, evidence of a structural review process, and evidence of proactive steps to improve the implementation of security measures.	**Not Yet**	Not all of the building blocks provided by e-SENS have reached a full technical maturity and scalability readiness - pilots did not provide a comprehensive documentation to claim accounting for changes, incidents, tests and exercises for improving the actual implementation of the security measures. However, solid basis for reaching this level are provided and the current cybersecurity analysis is also an evidence of a structural review and taking proactive steps towards recommendations for improving the implementation of security measures.

Table 23. Evaluation of sophistication level of e-SENS security measures according to ENISA descriptions

The levels are cumulative, so at level 2 the security measures and the evidence for level 1 are not repeated.

Risks are different for different providers and domains, and ascertaining which security objectives are important and which measures are appropriate depends on the context (the type of provider, the type of services offered, the assets in question, etc.). This affects the possibility to reach a certain sophistication level, but also implies that once such a level is reached it does not mean that the level stays valid regardless of the system evolution. The possibility of EIRA to be adapted to domain needs and to also evolve with the system under implementation speaks of its flexibility to retain the reached sophistication level.

This analysis wraps up the complementary view on the goal-based approach and complements the

cybersecurity evaluation of the EIRA with operational recommendations for securing the solutions based on EIRA.

3.6. Discussion

In addition to actively interacting with citizens and users on cybersecurity issues, governments, public administration and organizations are expected to enable end-users' reporting and feedback. However, as also shown by the analysis presented in this section, cybersecurity is not a domain or a sector-specific issue. Every entity that is part of a system (be it public administration, an organization or an ordinary user of services) is also concerned with some security aspect of that system. Information exchange platforms are crucial to the correct functioning of infrastructure and services that rely on interconnected information systems. Starting from the lowest level possible, training of both public administration, citizens and workers need to be enforced, since knowledge and behaviour of end-users is among the first lines of defence against cyber-threats. This is also integrated in the security objectives of the ENISA guidelines (SO6) in D2: Human resources security. e-SENS provides a set of recommendations reusable by the Member States and/or organizations in this regard.

However, not all of the recommendations for a secure system operation and maintenance can and should be addressed by e-SENS, imposing technical, legal, and organizational requirements is dealt with on a national or domain level. While desirable good practices may be part of its recommendations, mandatory security measures and properties are not.

In the e-SENS security context, addressing **availability**, conducting proper **risk management**, implementing adequate **human-oriented countermeasures** and accounting for the **trust establishment** recommendations are at the top of the priority list of future steps. The EIRA already offers a solid specification basis to address most of these requirements. Doing so would be a step further towards the calibration of the EIRA to the ultimate architecture needs.

With the security analysis presented in this deliverable, e-SENS meets one of the most important requirements for a secure system design - addressing security by design. Designing a methodology to both analyse the security measures provided by the implemented security mechanisms and integrating the outcomes of such analysis into the specifications allows for a technical person to cope more easily with the dynamics of security changes that a system may require. Furthermore, by enabling a non-technical person to understand the needs for implementing a certain security measure and the implications of not addressing it adds value in terms of usability of the system itself and for aligning the managerial requirements with the technical possibilities the system offers.

The evaluation of the EIRA technical maturity in Section 2 and the cybersecurity analysis in Section 3 can easily be joined to complement each other in getting the complete picture of the Evaluation of the EIRA in general. For example, if one takes the security analysis of the pilots through the RMIAS dimensions and goes back to the employment of the particular SATs and ABBs in a certain pilot, they can further extract information of the combination of ABBs that is able to meet a certain security goal. Furthermore, if one then looks at the security analysis of the EIRA's SATs, they can make comparative analysis of how the security aspects of the particular specifications and the implementations are aligned in a much broader, yet more granular context. Hence, all the analysis provided in this document are interconnected and complement each other, depending on the volume of information one needs and is willing to extract.

4. Conclusions

This deliverable has provided a structured evaluation of both the technical maturity and the security of the e-SENS Reference Architecture (EIRA).

The assessment of the technical maturity relies on a maturity model customized to the e-SENS Architecture, structured around the concepts of SAT and ABB. A standardised assessment process puts the model into operation and was conveyed to evaluate each SAT of the EIRA. A pilot survey was carried out to collect the required evidence supporting the measure of the technical maturity. All SATs reach the reliability level, meaning that their underlying specifications were thoroughly piloted through multiple implementations and that they are ready to be integrated in the design of specific solutions.

Besides the provisioning of evidence to support the technical maturity assessment, the pilot survey also contributed to the alignment of the reference architecture and the pilot solutions: a few gaps in specifications have been identified and filled through the change management process. Moreover, some emerging solutions were identified in the pilots and integrated within the EIRA as generic building blocks (Non-Repudiation, Local Attribute Provision and Federated Signing).

The evaluation of the Cybersecurity required the adoption and extension of a standard security model, RMIAS. The employment of the model in practice has led to a goal-based security analysis of each SAT, identifying how the technical specifications associated with the SAT contribute to meeting the security goals. In addition to this theoretical analysis, a pilot survey has collected the security practices employed in the pilots of the project. All of the pilots address an extended set of security goals and employ adequate means for their technical realization. However, the implementation of availability measures, proper risk analysis, and provision of human-oriented countermeasures require better alignment with the specifications.

This architecture evaluation has met its defined objectives of:

- Support Transfer of Ownership and Operations through a knowledge transfer of Building Block state-of-play: the architecture evaluation activities have contributed to bridge the gap between the reference architecture and the pilot solutions;

- Evaluate the Technical Maturity of the Building Blocks in relation to the Maturity Model in B.3 thereby contributing to an overall assessment of Building Block maturity: the technical maturity model was elaborated to cater with the components of the e-SENS Reference Architecture (SAT and ABB), and all components were evaluated according to the prescribed assessment process;

- Evaluate the e-SENS EIRA in relation to Cybersecurity, as stated in the Technical Annex: the cybersecurity evaluation assessed the compliance of the EIRA security aspects to an extended goals-based model. The relevant SATs and the adoption of the security principles from the pilots were evaluated and relevant security recommendations were extracted.

Annex I – e-SENS and the ENISA Guidelines on Security Measures

Cybersecurity goals play an important role in formulating the EU strategies and defining actions towards addressing them. The presented analysis is thus a contribution in that direction and an effort to bridge technical solutions with regulatory policies and standardisation.

Considering the fact that Information is the main security asset in e-SENS, and the only one in the context of EIRA, many of the security measures and objectives provided by ENISA are not realistic to be addressed. However, guidelines for the ones that are reasonable to be part of the security requirements in e-SENS are fully provided by the ENISA framework and will be elaborated further in this section. To do that, mapping of contextual and security traits between the e-SENS security needs and the ENISA provisions must be performed. This is presented in **Figure 18**, where the whole set of ENISA security objectives is also provided, divided in seven domains. The figure essentially shows the relevance of the ENISA security objectives in the context of e-SENS. The boxes represented in red denote relevance of that particular security objective (SO) for this analysis in the concrete domain (Dx); the green boxes represent the security objectives for which e-SENS may provide recommendations to Member States; and the transparent (white) boxes denote that the security objective is irrelevant for this analysis.

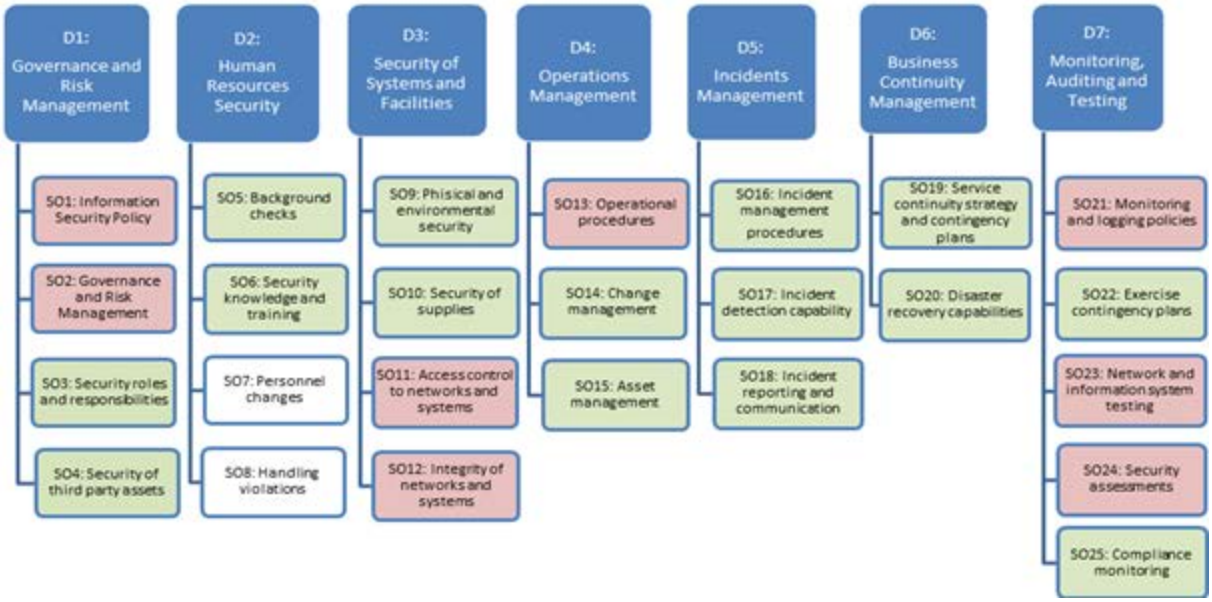

Figure 18. Relevance of the ENISA security objective in the context of e-SENS[41].

It is important to note here that the goals-based approach for cybersecurity evaluation offered by RMIAS already provides a partial threat-view on the security measures integrated in the EIRA and those implemented by the pilots. In addition, it is also the main reference model for the cybersecurity evaluation presented in this deliverable. Considering the fact that we are aiming to only complement the goal-based analysis with a threat-view on cybersecurity, mapping the contextual and the security

[41] Red denotes: Relevant for the analysis; Green denotes: e-SENS may provide Recommendations on these to Member States; White denotes: Irrelevant for the analysis

traits of the RMIAS to the ENISA framework would offer the necessary and sufficient practical and scientific rigor in accomplishing the task of a holistic cybersecurity evaluation.

In Annex II, the mapping of the RMIAS to ENISA's framework is presented. This mapping helped in extracting the specific guidelines and recommendations for the security measures that are required to meet the objectives relevant in e-SENS context.

Annex II – RMIAS and the ENISA Guidelines on Security Measures in e-Sens context

The mapping of the RMIAS to the ENISA technical guidelines essentially includes mapping of each of the RMIAS dimensions (Security goals, Information taxonomy, Countermeasures and Security system lifecycle) to the ENISA's framework of Security objectives divided by domain. This mapping is done by colouring the given table entry that lays at the intersection of an RMIAS row entry and an ENISA's column entry (in a matrix fashion). At the same time, the relevance to e-SENS context was also evaluated; this is denoted by colouring the particular entry in the same manner as presented in the previous section. Thus, a red entry denotes: Relevant for the analysis and for the particular point in the RMIAS; green entry denotes: Relevance for the particular point in the RMIAS and e-SENS may provide further Recommendations on this to the Member States; and a white entry denotes: Irrelevant for the analysis from RMIAS aspect and/or in e-SENS context).

As Information is the main asset addressed by the security mechanisms specified by the EIRA building blocks and implemented in the pilots, the mapping of the Information Taxonomy dimension of the RMIAS is performed in a more granular manner. In particular, the Information state sub-dimension is further divided into five additional dimensions: Creation, Processing, Storage, Transmission, and Destruction. These same dimensions were also part of the Security analysis of the pilots in section 3.7

The resulting table is thus a 25x25 matrix with an additional dimension for Relevance, represented with a colour, for a more convenient and compact view (**Table 24**). This additional dimension can be further fine-grained in different manners, either by another graphical representation, or by substituting it with numerical weights. Essentially, the table allows one to get a threat-view by domain of each of the goal-based dimensions and their sub-dimensions.

For example, based on the goal-based security analysis of the pilots in Section 3.4, it was detected that Availability is among the security goals that required better addressment. In the table that provides a threat-view of Availability, there are 19 security objectives relevant in the context of e-SENS across all of the 7 domains. Of those 19 objectives, 8 are mandatory for specification and implementation purposes, and for 11 e-SENS can provide recommendations to Member States or service providers. Depending on the specific domain pilot, a catalogue of security objectives that help to address Availability can be designed to help guide the specification and the implementation of the relevant security measures. Similar procedure can be taken to better address Governance and risk management that have also shown to be lacking in the pilots.

This cybersecurity analysis joins the benefits of a goal-based approach with the systemic nature of a threat-view on security management. It also helps to organize the security policies spread over multiple domains. Furthermore, it not only permits tracing possible contradictory security policy statements, but it also facilitates the identification of weak or omitted security policies. The Information Taxonomy and the Security Goals dimensions of the RMIAS provide a solid basis for a good coverage of situations in which security of information is needed, whereas the threat-based view complements these with a further granularity by domain and aspects of that particular domain. The security countermeasures classification of the RMIAS promotes consideration of different types of countermeasures for achieving the same security goals. Complemented with the more domain-specific security measures offered by the threat-based analysis may contribute to more cost-effective and efficient security solutions for both public administration and private organizations. Finally, the modularity of the presented analysis by security domain, objective, goal, countermeasure and additional systemic properties allows to pinpoint more easily possibilities for further improvement of

both the system/architecture under consideration (in this case the EIRA or the particular pilots) and the security mechanisms that are being integrated.

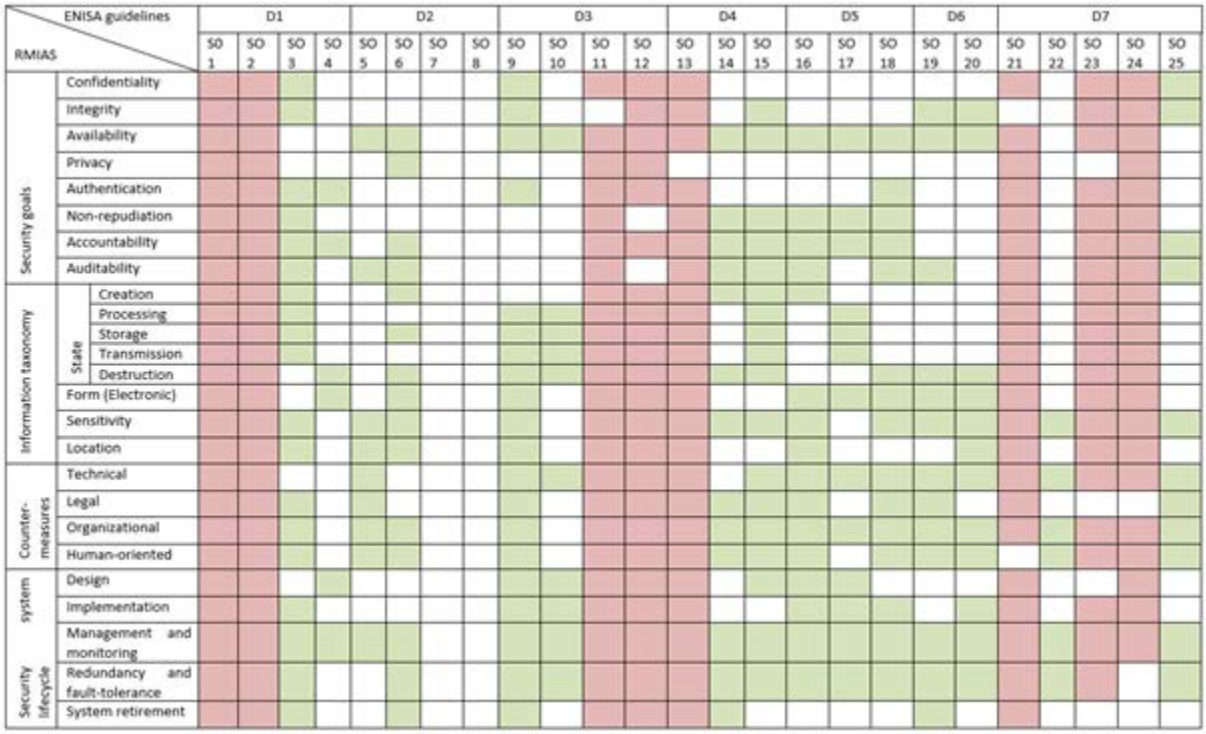

Table 24. Mapping RMIAS to ENISA guidelines by relevance for the e-SENS security mechanisms[42]

The fact that there is logical flow of the mapping procedure points to the possibility of formalizing the methodology into a more structured procedure that is domain-adjustable. Efforts of this kind are, however, out of the scope of this deliverable. Nevertheless, the possibility of such an undertaking is an argument of both the added value of the analysis presented in this deliverable and the EIRA's "ability" to lend itself to multi-domain and multi-aspect systemic analysis.

The threat-view on the cybersecurity evaluation is to a great extent subjective in the sense that the decision to assess a particular table entry as relevant or not depends on the analyst's expertise and experience. This was also pointed out as one of the drawbacks of a threat-based method. Therefore, in order to ensure the least bias possible, the evaluation has been reviewed by more experts who were involved in both the design of the specifications and in the implementations by the pilots. What is important as a result of the cybersecurity analysis, however, is the methodology itself, which not only is not subjective, but is based on rigorous standards and scientific approaches. Clearly, the results and the recommendations have to be further analysed and implemented by domain experts, as providing a domain set of security measure is out of the scope of this evaluation. The cybersecurity analysis can offer certain guidance in that regard.

Finally, it is worth noting that this table can further be checked for compliance with international standards by comparing it against the Mapping of ENISA's domains and security objective to

[42] Red denotes: Relevant for the analysis and for the particular point in the RMIAS; Green denotes: Relevance for the particular point in the RMIAS and e-SENS may provide Recommendations on these to Member States; White denotes: Irrelevant for the analysis from RMIAS aspect and/or in e-SENS context

international standards in Section 6 of the ENISA report. This also provided a vital argument in the efforts to determine the sophistication level of the security measures addressed by e-SENS, which is presented in **Table 23**, Section 3.5.2.

Annex III – EIRA questionnaire to pilots (template)

As per the Technical Annex of e-SENS proposal, WP6 is to "use experiences from the pilots to finalize a coherent ICT architecture to be ready for Transition into full scale production". In this regard, this is a questionnaire that[43] WP6 submits to pilot owners to gather feedback on the usage of e-SENS reference architecture – EIRA (i.e., ABBs and SAT). The goal is to represent each pilot according to the e-SENS EIRA meta-model. The answers to the questionnaire will be used for feeding the EIRA repository and the upcoming WP6 deliverables.

* Required

1.1. Pilot owners information

Q01. Please indicate your email address. *

Q02. Which pilot are you working on? *

1.2. eSENS Building Blocks

This section aims at understanding which Building Blocks of the eSENS reference architecture are in use within the pilot.

Q03. **SAT - eDelivery ---** Which Architectural Building Blocks (ABBs) for eDelivery are you using in the pilot? (select all that apply) *

- [ ] ABB - Message Exchange
- [ ] ABB - Capability Lookup
- [ ] ABB - Service Location
- [ ] ABB - Backend Integration
- [ ] We do not use SAT - eDelivery in our pilot

Q04. For each of the above selected ABBs, can you please provide a very short description of it in the pilot? (e.g., if you use ABB - Message Exchange, do you use it in a four-corner topology or in a point-to-point exchange?)

Q05. **SAT - eID ---** Which Architectural Building Blocks (ABBs) for eID are you using in the pilot? (select all that apply) *

[43] The questionnaire template document can be found at: https://www.jol.nrw.de/bscw/bscw.cgi/d8127403/WP6_WP5_Liaison_pilot_questionnaire.docx

- [ ] ABB - Authentication Exchange
- [ ] ABB - Attribute Provision
- [ ] ABB - Local Attribute Provision
- [ ] We do not use SAT - eID in our pilot

Q06. For each of the above selected ABBs, can you please provide a very short description of it in the pilot? (e.g., if you use ABB-Attribute Provision, can you indicate which attributes you are considering?)

Q07. **SAT - eSignature ---** Which Architectural Building Blocks (ABBs) for eSignature are you using in the pilot? (select all that apply) *

- [ ] ABB - eSignature Creation
- [ ] ABB - eSignature Validation
- [ ] We do not use SAT - eSignature in our pilot

Q08. For each of the above selected ABBs, can you please provide a very short description of it in the pilot? (e.g., f you use the ABB - eSignature Creation, can you please briefly describe the application being used?)

Q09. **SAT - eDocument** --- Which Architectural Building Blocks (ABBs) for eDocument are you using in the pilot? (select all that apply) *

- [ ] ABB - Document Provisioning
- [ ] ABB - Document Packaging
- [ ] ABB - Document Routing
- [ ] ABB - Document Annotation
- [ ] ABB - Business Rules Integration
- [ ] We do not use SAT - eDocument in our pilot

Q10. For each of the above selected ABBs, can you please provide a very short description of it in the pilot? (e.g., if you use the ABB - Document Provisioning, which activities do you instantiate according to the business needs of the pilot?)

Q11. **SAT - Traceability ---** Which Architectural Building Blocks (ABBs) for Traceability are you using in the pilot? *

- [ ] ABB - Non-Repudiation
- [ ] We do not use SAT - Traceability in our pilot

Q12. For each of the above selected ABBs, can you please provide a very short description of it in the pilot? (e.g., if you use ABB- Non-Repudiation, can you provide a brief description of the expected set of evidences emitted?)

Q13. **SAT - Semantics** --- Which Architectural Building Blocks (ABBs) for Semantics are you using in the pilot? (select all that apply) *

- [ ] ABB - Semantic Mapping Service
- [ ] ABB - Base Registry Identification and Access
- [ ] ABB - Core Vocabulary-Based Data Modelling
- [ ] ABB - Domain Specific Vocabulary Definition
- [ ] We do not use SAT - Semantics in our pilot

Q14. For each of the above selected ABBs, can you please provide a very short description of it in the pilot? (e.g., if the ABB - Core Vocabulary-based Data Modelling is used, can you please indicate which Core Vocabulary the pilot leverages?)

Q15. **SAT - Trust-Establishment ---** Which Architectural Building Blocks (ABBs) for Trust-Establishment are you using in the pilot? (select all that apply) *

- [ ] ABB - Trust Network – Mutually Recognized Certificates
- [ ] ABB - Trust Network – PKI
- [ ] ABB - Trust Network – Trust Service Status List
- [ ] We do not use SAT-Trust-Establishment in our pilot

Q16. For each of the above selected ABBs, can you please provide a very short description of it in the pilot? (e.g., if ABB - Trust Network - PKI is used, can you briefly describe the Trust Domain?)

Q17. Do you have recommendations on any additional functional enhancements to be provided to the ABBs or technical improvements for their specifications?

1.3. Specification usage

This section aims at gathering information on the use of the ABBs within the pilots, identifying possible gaps between what is described in the Reference Architecture and the actual use in the pilot.

Q18. Could you please indicate, motivating your answer, whether the used ABB Profiles (PR) fully meet the pilot requirements? *

Q19. With respect to the ABBs that have been previously selected, can you please point out whether you actually use all the features of each ABB specification? *

Q20. With respect to the previous question, are there any additional specifications you require in the pilot that are not provided in the current set of EIRA ABBs? *

1.4. Business Process

This section aims at understanding the business process used in the pilot and how the pilot sets up the ABBs previously indicated in order to meet specific business needs.

Q21. Which eService is being developed within the pilot? *

Q22. Can you outline the business process of the pilot where the ABBs selected in the previous answer are used? *

Q23. Can you outline the different steps of the business process, the involved components, and how the components interact with each other? *

Q24. Do you have a sequence diagram or any other diagram detailing the interactions between the used ABBs in the business process?

(If yes please send any reference to giorgia.lodi@agid.gov.it or eric.grandry@list.lu)

- [ ] Yes
- [ ] No

1.5. Security and Trust

The following questions are generic. There will be a more detailed questionnaire regarding Cyber-security, Security and Trust whose purpose will be to feed D6.4 and answer to the Objectives outlined in the Technical Annex.

Q25. Are any information confidentiality mechanisms used within the pilot? *

- [ ] Yes
- [ ] No
- [ ] Unknown

Q26. If Yes, could you state in what manner was the chosen mechanism employed? (e.g. encryption, passwords, verification, security tokens, etc.) *

Q27. Are any information integrity mechanisms used within the pilot? *

- [ ] Yes
- [ ] No
- [ ] Unknown

Q28. If Yes, could you state in what manner was the chosen mechanism employed? (e.g. hashing, file permissions, access controls, version controls, etc.) *

Q29. Are any information availability mechanisms used within the pilot? *

- [ ] Yes
- [ ] No
- [ ] Unknown

Q30. If Yes, could you state in what manner was the chosen mechanism employed? (e.g. redundancy, RAID, firewalls, DDoS attacks' prevention, etc.) *

Q31. In the pilot, are the above mechanisms used to counter specific cyber threats? *

- [ ] Yes
- [ ] No
- [ ] Unknown

Q32. If Yes, can you provide examples

1.6. Conformance and Interoperability Testing

This section aims at gathering information on the conformance and interoperability testing activities of the pilots for their eSENS SBBs. As a guidance please refer to the following descriptions:

- Conformance Testing verifies if an SBB complies with the eSENS ABB specification (E.g. For the ABB Specification "eSENS AS4", the SBB "Holodeck" took place in Conformance Testing activity)
- Integration Testing verifies if two or more SBBs that realize the same ABB specification work together properly (E.g. For the ABB Specification "eSENS AS4", the SBB "Holodeck" and the SBB "Flame" tested their interoperability on eSENS AS4 specification)

Q33. Can you please outline the ABB specifications that your Domain SBB's realize? ABB specifications include Foundation Architectures SP's and PR's (e.g. PR AS4 - Domibus) *

Q34. Can you please provide a short description of any participated Interoperability Testing activity between the SBB's used in your pilot and other vendor SBBs that realize the same ABB specification?*

Q35. Can you please provide a short description of any participated Interoperability Testing activity between your SBB and other vendor's SBBs that realize the same ABB specification? *

Q36. Can you please provide a short description of any other kind of Testing activities (e.g. Integration, System) that were carried out in your pilot? *

Annex IV – Cybersecurity questionnaire to pilots (template)[44]

This questionnaire aims to extract pilot experts' experience and expertise regarding the implementation of trust and security mechanisms within the pilots. The results from the processed questionnaire are aimed to feed the D6.4 deliverable and answer to the objectives outlined in the Technical Annex as well.

The Questionnaire employs RMIAS (Reference Model for Information Assurance and Security) as the most general reference model for Information Assurance and Security available.

Section 1 of 6: Pilot Information

Please state which pilot is your feedback referring to.

Section 2 of 6: Security Goals

This section aims to investigate how the security mechanisms implemented in your pilot (either technical, policy-related, organizational etc.) address general security goals.

1. Which of the following security goals were addressed by the mechanisms' design? (Select all that applies)

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Privacy
- ☐ Authentication and Trustworthiness
- ☐ Accountability
- ☐ Auditability
- ☐ Non-repudiation

2. Explain how were the selected goals addressed (e.g. Confidentiality: encryption, passwords, verification, security tokens; Integrity: hashing, file permissions, access controls, version controls, etc.)

3. Were the security mechanisms chosen with a particular threat model in mind?

[44] The questionnaire template document can be found at: https://www.jol.nrw.de/bscw/bscw.cgi/d8244167/Cybersecurity%20Questionnaire%20to%20Pilots.docm

- ○ Yes
- ○ No
- ○ Unknown

Section 3 of 6: Countermeasures

This section aims to explore the nature of the countermeasures and the means by which the security goals are to be achieved.

1. What technical countermeasures were employed to reach the security goals (e.g. encryption, authentication, authorization, etc.)?

2. What legal countermeasures were employed to reach the security goals (e.g. law, contracts, agreements, etc.)?

3. What organizational countermeasures were employed to reach the security goals (e.g. audit, policy, strategy, etc.)?

4. What human-oriented counter-measures were employed to reach the security goals (e.g. training, ethics, culture, motivation, etc.)?

Section 4 of 6: Information Taxonomy

1. In what state has the information been tackled by the mechanisms? (Select all that applies)

- ☐ Creation
- ☐ Transmission
- ☐ Storage
- ☐ Processing
- ☐ Destruction

2. Which of the following entities do you see being tackled by the employed mechanisms? (Select all that applies)

- [ ] Information
- [ ] People
- [ ] Processes
- [ ] Hardware
- [ ] Software
- [ ] Networks

Section 5 of 6: Trust

This section aims to collect information about the trust models employed by the pilots. The responses would complement the cyber-security report in order to provide a holistic overview of the security considerations by the e-SENS.

1. Are any trust mechanisms being implemented in the pilot?

- ○ Yes
- ○ No
- ○ Unknown

2. Choose the type of the trust model employed and denote the type of trust that is being ensured by that model?

☐ Direct trust (Mutual Key-Exchange)	Intradomain/Crossdomain →	*Denote the type of trust*
☐ Public Key Infrastructure	Intradomain/Crossdomain →	*Denote the type of trust*
☐ Central management (Trust List/Store)	Intradomain/Crossdomain →	*Denote the type of trust*
☐ Token-based (Usage of dedicated STSs)	Intradomain/Crossdomain →	*Denote the type of trust*
☐ SMP	Intradomain/Crossdomain →	*Denote the type of trust*

3. Are there any domestic (Member State) means (other than the aforementioned models) used to establish intradomain trust?

- ○ Yes
- ○ No
- ○ Unknown

4. If Yes, could you outline the employed means/protocols for trust establishment?

5. In case there are additional peculiarities with respect to the models employed, please denote them or share your experience: (e.g. implemented at the moment, but another model is also being considered for implementation; end-to-end trust establishment is enabled, etc.)

Section 6 of 6: General Assessment questions

This section is intended to capture the systemic properties of the implemented trust and security mechanisms.

1. Is the choice for employing the trust and security mechanisms based on an inherited infrastructure (found from previous projects)? (Capturing implementation context-details)

- Yes
- No
- Unknown

2. If Yes, state the infrastructure/projects and the inherited mechanisms provided by them.

3. Has the initial setting of the mechanisms been changed throughout the course of the pilot's testing/deployment? (Life-cycle trends' assessment)

- Yes
- No
- Unknown

4. If Yes, state any particularities related to it (e.g. reasons it was changed, whether it was a matter of the general system evolution, change of a particular context and requirements, etc.)

5. Do you envisage a low-frequency need for potential mechanisms' updates? (Sustainability assessment)

- Yes
- No
- Unknown

6. If No, what would you envisage the reasons might be?

7. Does a small change in the security mechanisms have big impact on the rest of the system? (Modularity and interconnectedness assessment)

- Yes
- No
- Unknown

8. If Yes, could you give an example of how a certain security aspect affects the general system?

9. Has redundancy been considered in the mechanisms' implementation?

- Yes
- No
- Unknown

10. If Yes, could you provide an example of how was this achieved?

11. Is the impact of a mechanisms' failure evaluated properly? (For Information Assurance)

- Yes
- No
- Unknown

12. If Yes, state in what manner was this achieved.

13. Has any risk management model been conveyed in the pilot?

- Yes
- No
- Unknown

14. If you can provide any figure or table representing the interactions among the considered risks, threats and vulnerabilities, please send it to **atanja@e5.ijs.si** or **eric.grandry@list.lu**.