



Smart Open Services for European Patients
Open eHealth initiative for a European large scale pilot of
Patient summary and electronic prescription

**epSOS
Requirement Consolidation II**

Appendix A

Document version	1.0
Last revision date	31/01/2013
Work package	WP5.2, KT5.2.5: Requirements Management
Distribution level	TPM
Status	Final
Editor	Oliver Kuttin
Contributor	Dr. Martin Hurch, Norbert Repas

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

History of Alteration

Version	Date	Type of editing	Editorial
0.1	2012-12-12	Initial Setup	ELGA
0.9	2012-12-31	Version submitted for Quality Review	ELGA
1.0	2013-01-31	Version issued after Quality Review	ELGA

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Table of Contents

1	Introduction	7
1.1	Scope	8
1.2	Objectives and expected benefits	9
1.3	Method.....	10
1.4	The ECCF Framework.....	11
1.5	What is a Requirement?.....	13
1.6	Readers' Guidance to Appendix A	15
	Appendix A	16
2	e1-FLD-29 Common Architecture, Design, Implementation	16
2.1	e1-FLD-31 Conceptual Perspective	16
2.1.1	e1-FLD-138 Architecture Principles	16
2.1.2	e1-FLD-139 Business Principle.....	16
2.1.3	e1-FLD-140 Data Principle.....	36
2.1.4	e1-REQ-1703 Security Principle	38
2.1.5	e1-FLD-141 Business processes	45
2.1.6	e1-FLD-142 Information Dimension	57
2.1.7	e1-FLD-191 High level architecture.....	64
2.2	e1-FLD-32 Logical Perspective	70
2.2.1	e1-FLD-145 Security architecture	70
2.2.2	e1-REQ-4602 REQ 3.3.17 HP-B authentication at NCP-B	116
2.2.3	e1-REQ-4608 REQ 3.3.23 Emergency Access through NCPs.....	116
2.2.4	e1-REQ-4618 REQ 3.3.26 Communication of identified exceptions.....	117
2.2.5	e1-REQ-4619 REQ 3.3.27 Feedback in case of identified exceptions.....	117
2.2.6	e1-REQ-4620 REQ 3.3.28 National helpdesk as part of feedback system	117
2.2.7	e1-REQ-4621 REQ 3.3.29 Error-message severity codes	118
2.2.8	e1-REQ-4622 REQ 3.3.30 Logging of errors	118

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.2.9	e1-REQ-1951 Traits Handshake central function	118
2.2.10	e1-REQ-1950 Taxonomy for the epSOS pivot format central function	119
2.2.11	e1-REQ-5298 Common Data Sources for NCP Operation	119
2.2.12	e1-REQ-4987 MTC Creation.....	120
2.2.13	e1-REQ-1949 Trusted Certificates	121
2.2.14	e1-REQ-4885 Trusted Node Infrastructure	121
2.2.15	e1-REQ-1948 National Contact Point Discovery Table	122
2.2.16	e1-REQ-4882 Service Discovery	122
2.2.17	e1-REQ-1721 Description of the flow of control	124
2.2.18	e1-REQ-4836 NCP-B Internet Front-End	134
2.2.19	e1-REQ-4841 General Considerations for Service Operations	134
2.2.20	e1-REQ-4847 Error Handling.....	136
2.2.21	e1-REQ-4851 Information messages and warnings	137
2.2.22	e1-FLD-169 Information Dimension	138
2.2.23	e1-FLD-149 Computational Dimension	138
2.3	e1-FLD-33 Implementable Perspective	139
2.3.1	e1-FLD-163 Information Dimension	139
2.3.2	e1-FLD-164 Computational Dimension	237
3	e1-FLD-28 Service specific Profile	240
3.1	e1-FLD-69 epSOS Semantic Implementation Guidelines.....	240
3.1.1	e1-FLD-193 Conceptual Perspective	240
3.1.2	e1-FLD-70 Logical Perspective.....	240
3.1.3	e1-FLD-71 Implementable Perspective	241
3.2	e1-FLD-68 Patient Identification.....	249
3.2.1	e1-FLD-72 Conceptual Perspective	249
3.2.2	e1-FLD-73 Logical Perspective.....	257
3.2.3	e1-FLD-159 Implementable Perspective	270
3.3	e1-FLD-67 Patient Consent	289
3.3.1	e1-FLD-74 Conceptual Perspective	289
3.3.2	e1-FLD-75 Logical Perspective.....	303

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.3.3	e1-FLD-167 Implementable Perspective	315
3.4	e1-FLD-66 Patient Summary	339
3.4.1	e1-FLD-76 Conceptual Perspective	339
3.4.2	e1-FLD-77 Logical Perspective	362
3.4.3	e1-FLD-78 Implementable Perspective	387
3.5	e1-FLD-65 eP/eD.....	419
3.5.1	e1-FLD-79 Conceptual Perspective	419
3.5.2	e1-FLD-80 Logical Perspective.....	445
3.5.3	e1-FLD-81 Implementable Perspective	488
3.6	e1-FLD-64 Healthcare Encounter Report (HCER) Service Specification.....	546
3.6.1	e1-FLD-82 Conceptual Perspective	546
3.6.2	e1-FLD-83 Logical Perspective.....	557
3.7	e1-FLD-63 Prescription Extended Service Specification: Medication Related Overview	574
3.7.1	e1-FLD-84 Conceptual Perspective	574
3.7.2	e1-FLD-85 Logical Perspective.....	583
3.8	e1-FLD-62 112 Additional Service Specification	597
3.8.1	e1-FLD-86 Conceptual Perspective	597
3.8.2	e1-FLD-87 Logical Perspective.....	606
3.9	e1-FLD-61 Patient Access Additional Service Specification	620
3.9.1	e1-FLD-88 Conceptual Perspective	620
3.9.2	e1-FLD-89 Logical Perspective.....	627
4	e1-FLD-250 Testing	642
4.1	e1-FLD-251 Conceptual Perspective	642
4.1.1	e1-REQ-5217 Main participation rules for test phases	642
4.1.2	e1-REQ-5216 Interactions among the epSOS test phases	643
4.1.3	e1-FLD-262 Test Phases	644
4.1.4	e1-FLD-275 Change management principles.....	663
4.2	e1-FLD-252 Logical Perspective	666

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.2.1	e1-FLD-265 Basic Requirements	666
4.2.2	e1-FLD-266 Engineering Level Requirements	670
4.2.3	e1-FLD-267 Sustainability Requirements.....	676
4.2.4	e1-FLD-264 Detailed Participation Criteria for the Test Phases (Conformance Gates)	677
4.2.5	e1-FLD-257 Test Items	682
4.2.6	e1-FLD-256 Computational Dimension	696

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

1 Introduction

Success rates of IT projects and longevity of resulting systems correlate with the completeness and quality of requirement specifications. Therefore, epSOS established the requirements management (RQM) support team as part of KT 5.2.5. Moreover, the web based enterprise requirements management software “Jamasoft Contour” has been acquired and deployed as the primary instrument of KT5.2.5, thus suiting the specific methodology described in chapter 1.3 and providing the technical framework for collaborative requirements documentation, structuring and tracing.

The complexity and rate of requirement changes in large projects provide a challenge to track the impact of changes, the execution of requirements and communication of requirements between work packages. Therefore a formalized system needs to be established to manage requirements in a structured way.

Although a very clear and complete requirements specification is rarely achieved in medium or large projects, the objective is to identify and track the substantial part of a project’s requirements throughout its lifecycle. Hence, epSOS Phase I requirements have been revised, consolidated and structured in close collaboration with corresponding deliverable authors and expert groups. On the one hand the semantic provisions of “*Keywords for use in RFCs to indicate Requirement Levels*” (RFC2119)¹ are utilized to foster the degree of requirements formalization, and on the other hand, the HL7 *Enterprise Conformance and Compliance Framework* (ECCF) has been adopted as the common structural model. Additionally, experience gained in the course of implementing epSOS Phase I requirements has been documented as supplementary, non-normative items.

¹ Request for Comments (RFC), a memorandum published by the Internet Engineering Task Force (IETF) representing standards and best current practices in context of web based software engineering.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

1.1 Scope

This document builds upon D5.2.1 “Requirements Consolidation I” and further includes requirements defined in the course of current epSOS phase II deliverables. The following deliverables have been processed, refactored and consolidated within D5.2.3:

- D1.4.1 “*EED SERVICES including use cases for all services*”
- D1.4.3 “*EED SERVICES including specifications for all services*”
- D2.1.1 “*Legal and Regulatory Requirements at EU level*”
- D3.1.2 “*Final definition of functional service requirements – ePrescription*”
- D3.2.2 “*Final definition of functional service requirements - Patient Summary*”
- D3.3.2 “*Final System Technical Specification*”
- D3.4.2 “*Common Components Specification*”
- D3.5.2 “*Semantic Services Definitions*”
- D3.6.2 “*Final identity Management Specification*”
- D3.9.1 “*epSOS Pilot System Components Specification*” and appendices
- D3.9.2 “*Testing Methodology, Test Plan and Tools*”
- D3.A.1 “*D3.A.1 EED DESIGN v.II.1.0*”
- D3.C.1 “*Proof of Concept Testing Strategy*” and appendices
- D5.2.1 “*epSOS Initial Scope Definition*”

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

1.2 Objectives and expected benefits

In most methodologies requirements management is understood as a discipline, not a project phase. Based on the terms of reference, its goal is to elicit, document and agree on the scope of what is and what is not to be built within a solution. This information is used by analysts, designers and programmers to design, specify and implement the solution, by testers for verification purposes and by project managers to plan and manage the project. All of these aspects are addressed in context of epSOS by specific workpackages as described within the epSOS description of work.

The explicit separation of requirements from specific solutions is recognized as indispensable to create a benchmark against which to measure the quality of the solution, or to compare alternative solutions.

Major goal of epSOS requirements management is to establish and maintain a common source of structured requirements in order to ensure consistency and completeness. Derived objectives are listed below.

- Maintain a common repository of epSOS requirements in a structured form
- Provide the basis for a methodical management of requirements across WPs
- Share requirements between WPs early in the process
- Provide communication of requirements to stakeholders
- Facilitate traceability of requirements from definition to implementation

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

1.3 Method

It is generally agreed that epSOS can be defined in multiple facets depending on viewpoint and stakeholder expectations as illustrated by the following example:

- From a regulatory viewpoint epSOS is a legal, technical and organizational blueprint for medical care processes that cross European borders.
- From a medical doctor's viewpoint epSOS is a medical document framework for encoding, transcoding and processing foreign patients' medical data in order to serve use case specific information needs.
- From an IT architects viewpoint epSOS is a document sharing platform that provides means for sending and fetching medical data across borders.

Consequently, requirements address the static and dynamic characteristics of an epSOS conceptual, logical or technical building block from a certain perspective. Moreover, the separation of concerns among business, information system architecture and technology implementation is indispensable to prevent mixing up domains of medical, legal, semantical and technology experts and to foster independent evolution of these domains as well as sustainability of epSOS. For these reasons, requirements in epSOS are structured in adherence to the *Enterprise Conformance and Compliance Framework* (ECCF), which is part of HL7 Service Aware Interoperability Framework.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

1.4 The ECCF Framework

The HL7-Enterprise Conformance and Compliance Framework² (ECCF) of the *Services-Aware Interoperability Framework* is a collector of artifacts that in combination explicitly – and potentially fully – describe from a number of different perspectives (viewpoints) the requirements related to various informational/static and behavioral/dynamic characteristics of a complex system. The following illustration depicts the ECCF as described by WP 3.A and adapted for requirements refactoring.

ECCF	Enterprise Dimension “Why” Policy	Information Dimension “What” Content	Computational Dimension “How” Behavior
Conceptual Perspective	Legal Policies, Business Cases, Scope	Conceptual Information Model	Architecture Principles, Business Principles, Security Principles
Logical Perspective	Requirements Catalogue	Logical Information Model	Service Architecture, Service Contracts, Service Operation
Implementable Perspective	Selected Standards and Profiles	Implementable Information Model, Implementation Guides	Service Specification, WSDLs, Bindings

The **ECCF dimensions** (based on ISO RM-ODP viewpoints³) focus on specific characteristics of the system and are categorised with the following criteria:

- *Enterprise Dimension* defines the business and reference context and is concerned with the organization's business objectives and processes. This dimension answers the question "why?" and refers to policies.

² HL7 Services-Aware Interoperability Framework: Canonical Version, Release 1.

http://www.hl7.org/documentcenter/public/ballots/2011MAY/downloads/SAIF_CANON_R1_I1_2011MAY.pdf

³ ISO standard Reference Model for Open Distributed Process IRM-ODP, ISO/IEC IS 10746 | ITU-T X.900)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

- *Information Dimension* is defined by one-or-more domain analysis models and is concerned with the nature of the information handled by systems. It also defines constraints on the use and interpretation of that information. This dimension answers the question "what?" and refers to information content.
- *Computational Dimension* is concerned with the functional decomposition of the system into a set of components each exhibiting a specific behavior and interacting at interfaces. This dimension answers the question "how?" and deals with behavior.

The **ECCF perspectives** reflect different levels of abstraction and are targeted at different expert groups:

- The artifacts in the *Conceptual Perspective* focus on the problem space rather than on a concrete solution. Conceptual-level artifacts sketch the essentials and core concepts of epSOS from a domain matter expert's point of view and as such define the holistic conceptual model of epSOS.
- Artifacts in the *Logical Perspective* represent traceable translations of conceptual artifacts into a form/format usable by and useful to architects and inward-facing analysts. This perspective covers the functional/logical requirements of epSOS and relates the epSOS solution space with its classes, services and operations.
- The *Implementable Perspective* represents the domain of developers, often in concert with dialogues with designers and/or architects. Note that the artifacts in this Perspective are not actual implementations, but rather implementable, i.e. contain all of the necessary technical bindings – e.g. data types, value sets, interface specifications, etc. – that will enable developers to implement the building blocks of the functional/logical specification by standards-based technical components

The separation of viewpoints and characteristics allows for a structured and manageable evolution of epSOS requirements as it minimizes overlaps and redundancies due to the introduction of explicit relations among requirements addressing different characteristics across several viewpoints. The disadvantage of this modularization and flexibilization is that such a model of requirements is not a documentation in the common sense of a serialized document with a clearly defined reading path. However, WP3.A as well as the semantic and security expert group introduce different flavors of documents which serialize related domain specific parts of the artifact network into linear documents (e.g. Implementation Guides, document request/retrieval mechanisms, Service Discovery).

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

1.5 What is a Requirement?

All requirements are defined by subject and domain matter experts collaborating within epSOS workpackages as well as expert groups. Depending on the specific domain, requirements can be basically classified as follows:

- Stakeholder need: a requirement from a stakeholder (e.g. epSOS MUST be compliant to European legislation)
- Feature: a service provided by the system, usually formulated by a business analyst; a purpose of a feature is to fulfill a stakeholder need (e.g. epSOS MUST provide functionalities to HCP-B that allow him to request medical data of patient-A)
- Supplementary requirement: another requirement (usually non-functional) that cannot be captured in use cases (e.g. Cross-border exchange of medical data MUST minimize the amount of personal data that is disclosed and processed in both country A and B)
- Test case: a specification of test inputs, execution conditions, and expected results (e.g. workflow test which tests a complete use cases as performed in the course of connectathon and PPT test phases)

In adherence to the ECCF model each requirement is represented at different levels of abstraction which have to be considered by different expert groups. First, conceptual requirements are defined at an enterprise level serving as a foundation building of epSOS with respect to legal, semantical, architectural and security aspects. Subsequently, these high-level requirements are translated by IT-architects and inward-facing analysts to logical/functional specifications of epSOS defining its classes, services and operations. Finally, the implementable level of ECCF encompasses all technical bindings (e.g. data types, value sets, Web Service Description Language (WSDL) specifications) which allow for implementation of the logical building blocks in standard based fashion.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

In software-engineering and law making it is common to separate out normative texts to assist interpretation of the correct meaning. Consequently, normative requirements and non-normative additions are structured within the Contour requirements management tool by means of two distinct information classes, i.e. "Requirement" and "Note". Examples for normative and informative information items:

<i>Normative</i>	<i>Non-normative</i>
Need	Solutions
Feature	Intro/Abstract/Summary
Test case	Examples, Explanations

The following check list has been (and should be in the future) considered for requirements elaboration, definition and review:

- Does the requirement specify WHAT to do? (platform independent)
- Do the requirements describe high level features or capabilities of the solution with respect to the following topics:
 - o Outputs that should be produced by the solution;
 - o Inputs that will enter the solution;
 - o Logical files that must be maintained by the solution;
 - o Entities and relationships that will be in the logical files of the solution;
 - o Interaction patterns that can be used with the solution;
 - o Interoperability aspects of the solution
 - o Key algorithms that must be supported by the solution;
 - o Use cases that shall be implemented by the the solution;
 - o Access control principles;
 - o Behaviour of the the solution in case of invalid input and processing errors;
 - o Laws and regulations that impact the the solution;
 - o Standards the the solution must adopt and comply with;
 - o Information security objectives like confidentiality, integrity, availability, accountability and privacy;
 - o Performance/Scalability/Sustainability

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Factors not considered as part of requirement management in epSOS:

- Quality levels in terms of defects, reliability, and ease of use criteria;
- Risk factors like termination, delays, overruns;
- Test Cases, which are managed within Gazelle® test management tool
- Project cost and life expectancy;
- Release frequency for new features and repairs;
- Delivery type such as OSS, SaaS etc.

1.6 Readers' Guidance to Appendix A

First, chapter 2 states the foundational building of an epSOS NCP with regard to common principles of design, architecture, interaction patterns as well as related legal, semantic, and security frameworks. The structure of chapter 2 reflects the approach underlined in chapter 1.4.

Second, chapter 3 comprises of the epSOS services, which build upon the NCP fundaments described in chapter 2 and fulfill corresponding requirements. However, these services are clearly differentiated by their functional requirements and derived, service specific constraints on the architectural, semantic and security related building blocks. Specified services are as follows:

- Patient Identification
- Patient Consent
- Patient Summary (PS)
- ePrescription/eDispensation (eP/eD)
- Healthcare Encounter Report (HCER)
- Medication Related Overview (MRO)
- 112 Additional Service Specification
- Patient Access Additional Service Specification (PAC)

The structure of chapter 3 reflects the approach underlined in chapter 1.4

Finally, chapter 4 covers epSOS testing principles, describes test phases, corresponding relations and interactions among them as well as participation and exit criteria. Moreover, this chapter structures engineering level requirements for the test bed addressing document, messaging and Business (Workflow) layer validation on the logical perspective.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Appendix A

2 e1-FLD-29 Common Architecture, Design, Implementation

2.1 e1-FLD-31 Conceptual Perspective

2.1.1 e1-FLD-138 Architecture Principles

2.1.2 e1-FLD-139 Business Principle

2.1.2.1 e1-REQ-2202 L-DP-01 Transmission of data to third countries

A standard form contract which incorporates the necessary elements of the FWA, the required SCC as well as the specific clauses pertinent to the bilateral relationship, to be signed bilaterally by each PN piloting with Turkey, shall be drafted.

2.1.2.2 e1-REQ-2205 L-DP-02 Patient information notice as a prerequisite for explicit patient consent

The Patient Information Notice must be sufficient to enable the patient to give explicit consent to the processing of data in accordance with the requirements stated in the Data Protection Directive (D 95/46/EC) and the Patients' Rights Directive (D 2011/24/EU)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.3 e1-REQ-2206 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-3869 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-4539 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-5097 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-5098 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-5103 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-5104 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-4564 NFR09- Trust between countries

epSOS agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations must be secured and codes of conduct as part of the epSOS Information Governance must be elaborated.

2.1.2.4 e1-REQ-2208 L-DP-04 Migration to common eID EU approach

epSOS shall consider the opportunity to migrate to the common eID EU approach foreseen in Article 14 of the PRD.

2.1.2.5 e1-REQ-2209 L-DP-05 Authorization of Health Professionals

epSOS shall consider the opportunity to incorporate provisions for authorization of health professionals in compliance to the PRD.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.1.2.6 e1-REQ-2210 L-DP-06 Patient Consent accounting for purpose and manner of data processing

Related to e1-REQ-1970 Consent Registration

Purpose and manner of the data processing must be covered by the patient's consent regarding all epSOS Services.

2.1.2.7 e1-REQ-2217 L-DP-07 Proportionality and purpose limitation

Related to e1-REQ-1976 Needs-to-Know-Principle

Each query about the personal data available through epSOS should be based on a real need of access to the specific information and no personal data returned by country B shall be stored at the NCP.

2.1.2.8 e1-REQ-2203 L-HS-01 The epSOS NCP within the Patients' Rights Directive

Against the backdrop of the efficiency requirement (Art. 12/2/d PRD) an analysis of the duties of the epSOS NCP in the framework of the PRD including opportunities to co-locate the PRD and epSOS functions must be performed.

2.1.2.9 e1-REQ-2204 L-HS-02 International interoperability epSOS agreements on security levels, common eID measures and other relevant issues

Member States shall facilitate cooperation in cross-border healthcare provision at regional and local level as well as through ICT and other forms of cross-border cooperation.

The Commission shall encourage Member States, particularly neighbouring countries, to conclude agreements among themselves.

2.1.2.10 e1-REQ-2219 L-HS-03 Electronic cross border access to medical information

The epSOS PS shall be aligned/influence the development of guidelines on a non-exhaustive list of data that are to be included in patients' summaries and that can be shared between health professionals to enable continuity of care and patient safety across borders.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.11 e1-REQ-2207 L-HS-04 Health care providers duties and responsibilities regarding informed choice

epSOS healthcare providers shall notify on availability of epSOS services and report on performance data and shall provide clear information on use of epSOS for patients.

2.1.2.12 e1-REQ-2211 L-HS-05 Manner and form of the right to access to health information by Patient

Related to e1-REQ-2178 PAC FR01 Patient Access basic requirement

Access for patients to their records MUST be facilitated as required by the PRD. Patients MAY be given a print out of parts of the record.

2.1.2.13 e1-REQ-2213 L-HS-06 Updating of patient records

The relevant service specification must take into account national operational approaches for updating of patient summaries.

2.1.2.14 e1-REQ-2216 L-HS-07 Interoperability of ePrescriptions

epSOS shall adhere to/influence the development of guidelines foreseen under Art. 14 PRD supporting the Member States.

2.1.2.15 e1-REQ-2212 L-LI-01 Traceability

Related to e1-REQ-1980 Traceability and Exercise of Patient Information Rights

All transactions shall be logged and an audit trail created and stored. A patient should also have the right to see the log and know who used or saw his medical data.

2.1.2.16 e1-REQ-2214 L-LI-02 Auditable processes for production of the MTCs

epSOS shall elaborate commonly accepted and auditable processes for production of the MTCs.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.2.17 e1-REQ-2215 L-LI-03 Clinical governance concerning data quality

epSOS shall deal with clinical governance issues to the appropriate depth as far as issues of quality of data (data coding) is concerned.

2.1.2.18 e1-REQ-4585 REQ 3.3.0 Modifications to medical data received from Country-A by HP-B

Related to e1-REQ-4600 REQ 3.3.15 eP data are not modifiable by country B

In context of epSOS information is exchanged but not shared. Any HP-B MAY NOT modify an original document received from Country-A.

2.1.2.19 e1-REQ-4587 REQ 3.3.2 NCP creates secure link between epSOS and national domain

A National Contact Point (NCP) acts as a legal entity which creates a secure link between the epSOS trust domain from the national trust domain. It is the only component that has an identity in both domains. NCP of country A (NCP-A) shall act as a data provider through its Inbound Gateway, providing the medical documents located in country A. NCP of country B (NCP-B) shall act as a data consumer through its Outbound Gateway, used by HP in country B to access medical documents provided by NCP-A.

2.1.2.20 e1-REQ-4588 REQ 3.3.3 Single NCP per PN

A single NCP MUST be provided by each PN within epSOS. The NCP shall act as a gateway between the "epSOS side" (which exists in between 2 NCPs) and the "national side" (which exists only within PN). A trusted domain is set up between NCPs and its management is in scope of epSOS.

2.1.2.21 e1-REQ-4590 REQ 3.3.5 Synchronous Communication

Related to e1-REQ-1993 Scalability wrt Availability, Performance and Throughput

Communications MUST be processed between gateways in a synchronous fashion.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.22 e1-REQ-4616 3.3.6.1 Session initialization by NCP-B

In country B, a session in epSOS SHALL consist:

- a HCP identity assertion
- a patient identifier that is accepted by country A
- a treatment relationship assertion

2.1.2.23 e1-REQ-4617 3.3.6.2 Session initialization by NCP-A

In Country A, a session MAY be set up for the following tasks:

- an internal session for performance reasons but this session is not visible outside of NCP-A (i.e. in the PN health information service).
- the possibility is left to PN decisions but it has to be noted that sessions may recover load-balancing and fall-over capabilities.

2.1.2.24 e1-REQ-4593 REQ 3.3.8 Patient Data is univocally identifiable

Patient data belong to PN's health information systems: each shall be identifiable univocally (it is a national responsibility) and may implement gateways for in-out-bounds transactions (again, a national responsibility).

2.1.2.25 e1-REQ-4595 REQ 3.3.10 Patient data within existing national infrastructure

Patient data (i.e. original, source data) shall be kept within their national existing infrastructure. PoC in country B may store the received and generated health data only to be kept for purposes defined by the current legislation in country B.

2.1.2.26 e1-REQ-4601 REQ 3.3.16 Transformation at NCP-A

Transformation of the original medical documents to the epSOS pivot format should be initiated and signed under the responsibility of NCP-A.

Privacy law of some PNs may require that data transformation is performed not in the NCP, but in the system where the information is kept or in the system where the information is exploited. The original document (PDF document compliant to PDF/A-1b) MUST be sent to NCP-B with the transformed document (CDA format) for safety and security reasons.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.26.1 e1-TXT-725 Note

It is a national responsibility to do the mapping based on the pivot format, not an epSOS responsibility.

2.1.2.27 e1-REQ-4606 REQ 3.3.21 Common epSOS resources

Related to e1-REQ-1948 National Contact Point Discovery Table

Related to e1-REQ-1950 Taxonomy for the epSOS pivot format central function

Related to e1-REQ-1951 Traits Handshake central function

Related to e1-REQ-1949 Trusted Certificates

Related to e1-REQ-5298 Common Data Sources for NCP Operation

The following epSOS resources MUST exist in the same state for every NCP for the cross-country system to operate:

A Routing Table in order to locate NCPs within epSOS,

A list of the epSOS Trusted Certificates,

A Taxonomy for the epSOS pivot format and the epSOS Master Value Set Catalogue and Master Translation Catalogue. Those services MAY be duplicated on the national side but SHOULD be maintained centrally,

Information about the requirements of each country and acceptable forms of patient identification and consent,

Support material for development and testing.

2.1.2.28 e1-REQ-4443 REQ 3.6.35 Access to patient's health data

Related to e1-REQ-4441 Process “HP accessing health data of a patient” (with given consent)

Any participating country must establish organisational procedures and functionalities to support the described process of accessing health data of patients from Country B.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.29 e1-REQ-4446 REQ 3.6.37 Processes for emergency cases

Related to e1-REQ-4608 REQ 3.3.23 Emergency Access through NCPs

Related to e1-REQ-4445 Process “HP accessing health data of patient” (emergency case)

Related to e1-REQ-4444 REQ 3.6.36 Transmitted attributes in health data access attempts

For emergency access, special procedures must be designed. The HP requesting an emergency access must specifically and doubtlessly state his intention and reason for the emergency data access request. This information must be forwarded to Country A as decision support for the access control decision.

2.1.2.30 e1-REQ-4447 REQ 3.6.38 County A decides in emergency cases

Related to e1-REQ-4981 Process Access Control with epSOS Use Cases

Related to e1-REQ-4445 Process “HP accessing health data of patient” (emergency case)

Country A must be the place, where the particular emergency access decision is taken.

2.1.2.31 e1-REQ-4448 REQ 3.6.39 Laws regulating emergency cases

WP 2.1 must check the different laws in the PN and to define the process of emergency access for epSOS LSP.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.2.32 e1-REQ-1960 Compliance to European Legislation

Related to e1-REQ-8 Context within interoperable European eHealth Strategy

Related to e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-1962 Autonomy of National Infrastructures

Related to e1-REQ-1978 Data Integrity

Related to e1-REQ-1979 Data Minimization

Related to e1-REQ-1976 Needs-to-Know-Principle

Related to e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-1977 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

epSOS MUST be compliant to European legislation.

epSOS MUST in particular consider:

directives on patient privacy and patient rights

... (to be completed by WP2.1)

2.1.2.33 e1-REQ-1961 Patient Safety

Related to e1-REQ-10 Maintain patient safety

Related to e1-REQ-1978 Data Integrity

Related to e1-REQ-1984 Data Origin and Data Authenticity

Related to e1-REQ-1985 Patient Data Assignment

Related to e1-REQ-1988 Peering Original Document

epSOS MUST NOT impose any risks on patient safety.

Implications:

epSOS MUST implement appropriate policies and technical means to reduce and manage risks on patient safety.

Of specific concern MUST be data accuracy, integrity, currentness and completeness which cannot be fully guaranteed by epSOS (and heavily depends on the initial level of security as provided by country-A) and therefore MUST be accomplished by epSOS usage policies.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.34 e1-REQ-1962 Autonomy of National Infrastructures

Related to e1-REQ-1960 Compliance to European Legislation

Related to e1-REQ-11 EU-wide applicability

Related to e1-REQ-1965 IT-Systems directly controlled by HPs

Related to e1-REQ-1963 National Contact Points (NCPs)

epSOS PNs MUST NOT be forced to modify their existing national eHealth infrastructures or legislations in order to participate in epSOS.

epSOS MUST be specified, implemented and defined in a way that allows all PNs to connect their existing national eHealth infrastructures to epSOS without requiring alterations in existing technology, data semantics and legislation.

epSOS MUST NOT define technical solutions that exclude PNs from taking part in epSOS pilots and operations under the legal umbrella of epSOS.

epSOS cross-border data sharing services SHOULD be as transparent for affected human entities as possible, in a way that the MUST NOT enforce changes in medical and/or administrative processes at the affected points of care.

Implications:

epSOS architecture and design SHOULD NOT make any assumptions on services, processes and technologies which are deployed within national infrastructures – unless such assumptions reflect agreed requirements on secure end-to-end processes.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.2.35 e1-REQ-1963 National Contact Points (NCPs)

Related to e1-REQ-1962 Autonomy of National Infrastructures

Related to e1-REQ-1964 Trust Relationship between National Contact Points (NCPs)

.... some well aligned phrasing on the legal role of NCPs and their representation as gateways on the architectural level ...

Following the principle of “complete mediation” there MUST NOT be any defined epSOS transaction on medical data that bypasses NCP-A and/or NCP-B. This implies that identifiable medical data can only leave and enter a national infrastructure through a national gateway (NCP).

2.1.2.36 e1-REQ-1964 Trust Relationship between National Contact Points (NCPs)

Related to e1-REQ-1963 National Contact Points (NCPs)

A node that can be identified and authenticated as a country’s NCP MUST be assumed to be trustworthy wrt the proper implementation of all epSOS policies and requirements. This trust assumption MUST hold as well for all epSOS services that are provided by such a trusted NCP node.

NCP identification and authentication MUST be of sufficient strength and accuracy. It MUST be implemented by technical means which reflect the current state of the art in node and service authentication. NCPs MAY be targets to security threats. Therefore epSOS assessments on threats and risks MUST consider that NCP security means may be weakened or that NCP operators may misuse their role.

2.1.2.37 e1-REQ-1965 IT-Systems directly controlled by HPs

Related to e1-REQ-1962 Autonomy of National Infrastructures

IT-Systems which are directly controlled by an HP MUST be assumed to be trustworthy in that they provide an sufficient level of data privacy, data integrity, data availability and data authenticity. This trust assumption MUST hold as well for all data processing services that are operated on such a system.

epSOS assessments on threats and risks MAY ignore possible threats on data security and privacy for data that is stored/processed in an HP's IT system as the maintenance of secure HP environments is out of the scope of epSOS. HP s' IT systems SHOULD be considered as (the only) fully secure environments. epSOS SHOULD NOT define or imply technical means for protecting data privacy and security within such environments.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.38 e1-REQ-1967 Country-A as Primary Source

Related to e1-REQ-1972 Patient Access

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Country-A MUST be considered as the primary and only place for requesting up-to-date, consistent and approved medical data of patient-A.

Country-A is responsible for keeping the medical information of their patients up-to-date. epSOS does not make any assumptions on how medical data is managed within a country A. epSOS SHOULD provide means for supporting country-A in keeping their patients' data up-to-date, consistent and complete. epSOS service operations and contracts SHOULD be content agnostic; e.g. a request for a patient's medication summary SHOULD – from a logical and implementable perspective – be the same as a request for a patient's ePrescriptions.

2.1.2.39 e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-2091 Element <translation>

Related to e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Related to e1-REQ-2090 Recording of transcoded/translation data

Related to e1-REQ-2092 Reference coded system used in Country A

Synchronized with e1-REQ-3871 Semantic Interoperability of Structured Clinical Content

Synchronized with e1-REQ-4544 Semantic Interoperability of Structured Clinical Content

Synchronized with e1-REQ-5102 Semantic Interoperability of Structured Clinical Content

Synchronized with e1-REQ-5127 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-4953 TransformationManager

Medical information shared among countries MUST be understandable (in the correct context) for the receiver. HP-B MUST be enabled to view and/or process medical documents encoded in a way that best matches the document structure and clinical terms that are commonly used in country-B.

Implications:

epSOS MUST provide semantic services that allow for translation/mapping of clinical terms. epSOS SHOULD use a common pivot schema and terminology set in order to limit the number of mappings that have to be defined and maintained.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.40 e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

Related to e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Related to e1-REQ-4935 Request Message

Synchronized with e1-REQ-3865 Structured Information and Semantic Compliance

Synchronized with e1-REQ-4543 Structured Information and Semantic Compliance

Synchronized with e1-REQ-5099 Structured Information and Semantic Compliance

Synchronized with e1-REQ-5101 Structured Information and Semantic Compliance

epSOS MUST define the structure and semantics of all document types which are required to be shared cross-border within epSOS use cases (pivot schema and common terminologies).

It is the responsibility of each PN to preserve the semantics of original data when this is transformed and transcoded into the common epSOS format as defined for the respective document type. Transformation services within a country and epSOS semantic services should guarantee the smoothest semantic transformation, keeping the meaning and the value of the source document, considering the liability for the transformation, and assuring the reproducibility of the semantic transformation.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.2.41 e1-REQ-1991 Extensibility of the Use Cases

Related to e1-REQ-1996 Continuous Improvement

Related to e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Related to e1-REQ-1966 Request for Medical Data

Related to e1-REQ-1993 Scalability wrt Availability, Performance and Throughput

epSOS architecture MUST allow for an efficient extension of existing use cases and for a simplified definition of new use cases within the defined functional scope. epSOS MUST be content agnostic by being able to exchange medical documents of different types. The architecture SHOULD allow for a parameterization of requests that allows an HP-B to express which kind of patient-A data he needs (e. g. patient summary or active prescriptions).

Implications:

epSOS service operations and contracts SHOULD be content agnostic; e.g. a request for a patient's medication summary SHOULD – from a logical and implementable perspective – be the same as a request for a patient's ePrescriptions.

2.1.2.42 e1-REQ-1992 Use of Standards

Related to e1-REQ-1993 Scalability wrt Availability, Performance and Throughput

epSOS MUST make use of established standards wherever suitable. The use of existing standards MUST be envisioned. The extension/adaptation of existing standards SHOULD be preferred for the definition of a proprietary solution. epSOS extensions to existing standards MUST be discussed with the respective standardization bodies and SHOULD be integrated with these standards.

Implications:

The functional design of epSOS SHOULD consider properties of established solutions.

Specific epSOS features that cannot be mapped on existing standards SHOULD be re-assessed on whether they are really needed or could be substituted by modifications in the business processes.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.43 e1-REQ-1996 Continuous Improvement

Related to e1-REQ-1991 Extensibility of the Use Cases

Related to e1-REQ-1993 Scalability wrt Availability, Performance and Throughput

epSOS services (including processes, deployment, interfaces) MUST be suited to be continuously improved with respect to changing user behavior. Usage processes, service usage patterns and user feedback MUST be tracked continuously in order to detect architectural weaknesses, inappropriate design decisions and inappropriate technologies.

Implications:

epSOS services MUST provide data for the continuous evaluation of epSOS usage patterns and their impact on the running solution.

2.1.2.44 e1-FLD-277 Clarifications to the FWA

2.1.2.44.1 e1-TXT-885 Note

Scope

There are many types of policies in epSOS including for handling deliverables, financial issues, communication etc. This document is focusing ONLY on those that represent PN agreements in terms of the legal, information security and information quality requirements in the form of epSOS specific safeguards to be reflected in the national policies for data protection, information security and data quality.

epSOS policies have been captured in the FWA and the epSOS Security and Audit policy. These policies have been put to strain test (i) by epSOS piloting preparation and launch and (ii) by the WP29 review and subsequent consultation with WP29 subgroup on eHealth chair. Both validation activities have resulted in a set of Recommendations which have been carefully considered and reflected in this proposal. Both sets of Recommendations have been presented and discussed in the PSB.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.1.2.44.2 e1-FLD-278 DATA PROTECTION AND CONFIDENTIALITY

2.1.2.44.2.1 e1-REQ-5277 Art. 1

The articles of the Framework Agreement and its annexes shall be transposed into:

- a. (where necessary) Contracts under applicable national law to establish epSOS NCPs and
- b. (where necessary) Contracts under applicable national law to designate Points of Care from within existing Healthcare Providers as epSOS Points of Care.

2.1.2.44.2.2 e1-REQ-5278 Art. 2

The terms of the FWA and its annexes may be modified during transposition into local contracts and guidelines only in so far as it is necessary to do so in order to comply with local law or custom.

2.1.2.44.2.3 e1-REQ-5279 Art. 3

The contractual agreements established at national level to create the NCPs shall be certified as conformant to epSOS principals by the Project Steering Board.

2.1.2.44.2.4 e1-REQ-5280 Art. 4

All data contained in medical documentation, in electronic health records and in EHR systems are “sensitive personal data” and therefore subject to Article 8 of the Directive.

2.1.2.44.2.5 e1-REQ-5281 Art. 5

The processing of healthcare data must have a clear legal basis. In the absence of other legitimate grounds, this can be the data subject’s two-step explicit consent (first for participation in general and then in the case of the concrete treatment/dispensation).

2.1.2.44.2.6 e1-REQ-5282 Art. 6

Where the country of affiliation requests (A) and the country of treatment (B) can make it feasible, it is possible to allow patients to give also their first consent in country B, for instance in a secure way over the Internet.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.44.2.7 e1-REQ-5283 Art. 7

Processing of personal and sensitive data can be justified without second consent in country B if it is necessary to protect the vital interests of a data subject or of another person if in the emergency case the data subject is physically or legally incapable of giving his consent.

- a. In this event the patient should be informed about the override of consent upon leaving the PoC including details of access OR
- b. Patient should be provided access to epSOS audit trails

2.1.2.44.2.8 e1-REQ-5284 Art. 8

The processing of personal data must be strictly limited to the minimum which is necessary for the fulfillment of the epSOS purposes which must be specified, explicit and legitimate.

2.1.2.44.2.9 e1-REQ-5285 Art. 9

Data in the log files is to be stored for the purposes of the pilot and for litigation purposes up to a maximum of 10 years as defined in the Grant Agreement.

2.1.2.44.2.10 e1-REQ-5286 Art. 10

Each query about the personal data available through epSOS should be for a real need of access to specific information related to the care or treatment to be provided or the medicine to be prescribed or dispensed in a particular case.

2.1.2.44.2.11 e1-REQ-5287 Art. 11

All data controllers handling epSOS data must notify the competent supervisory authority in accordance with the national legislation, regardless of whether the data subjects are nationals or residents of another PN and irrespective of whether the data handled originate from data controllers in other PNs.

2.1.2.44.2.12 e1-REQ-5288 Art. 12

The pilot sites shall apply all epSOS specific security requirements and provide evidence of conformance when requested by the NCP for the purposes of monitoring and audit.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.1.2.44.2.13 e1-REQ-5289 Art. 13

Duplicate with e1-REQ-5295 Art. 19

Before admitted into the epSOS pilot, an epSOS pilot site shall complete and submit to its national NCP the Initial Audit Report for further assessment and approval by epSOS function with the relevant mandate by the PSB.

2.1.2.44.2.14 e1-REQ-5290 Art. 14

Duplicate with e1-REQ-5296 Art. 20

Subsequent full Audits by the NCP shall take place according to epSOS Audit policy (FWA, Annex II, par. 1.4)

2.1.2.44.2.15 e1-REQ-5291 Art. 15

A data subject should be able to address questions about access and demands for rectification/erasure/blocking to any of the controllers as well as to any other body involved in the exchange of information within epSOS. A demand to access or for the rectification/erasure/blocking of data which is given to an epSOS partner who does not handle data about the data subject, should be forwarded to the data controller in charge within the epSOS system even if this relevant controller is established in another PN.

2.1.2.44.2.16 e1-REQ-5292 Art. 16

A common epSOS website should inform on the specific rights of data subjects according to the different legislations of all the participating nations. The information on the website should clearly specify the rights, conditions and practicalities according to the national legislation of each PN.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.1.2.44.3 e1-FLD-279 INFORMATION SECURITY

2.1.2.44.3.1 e1-REQ-5293 Art. 17

A high level of IT-security is necessary for epSOS. Especially the following measures and arrangements are necessary in order to take full account of security principles which follow from the Directive and the specific risks related to the processing of personal data in epSOS:

- a. All staff implementing the project should be provided with clear-cut, written instructions on how to appropriately use the epSOS system in order to prevent security risks and breaches.
- b. Suitable arrangements should be made in using the Patient Summary and prescription storage and archiving systems to protect the data against unauthorized access, theft and/or partial/total loss of storage media.
- c. For data exchanges, secure communication protocols and end-to-end-security must be adopted.
- d. Special attention must be paid to adopting a reliable and effective electronic identification system that provides the appropriate level of assurance (of both participating staff and patients) in compliance with eHN decisions.
- e. The system must be capable to correctly record and track in an auditable way the individual operations that make-up the overall data processing.
- f. Unauthorized data access and/or changes should be prevented when the back-up data are transferred and/or stored.
- g. With regards to the e-prescription services, additional measures should be deployed in order to ensure that when epSOS pharmacists retain records of dispensed prescriptions these records are used exclusively for the legal purposes documenting the dispensation.
- h. In emergency situations, any access should be logged and subject to audit.

2.1.2.44.3.2 e1-REQ-5294 Art. 18

The pilot sites shall apply all epSOS specific security requirements and provide evidence of conformance when requested by the NCP for the purposes of monitoring and audit.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.2.44.3.3 e1-REQ-5295 Art. 19

Duplicate with e1-REQ-5289 Art. 13

Before admitted into the epSOS pilot, an epSOS pilot site shall complete and submit to its national NCP the Initial Audit Report for further assessment and approval by epSOS function with the relevant mandate by the PSB.

2.1.2.44.3.4 e1-REQ-5296 Art. 20

Duplicate with e1-REQ-5290 Art. 14

Subsequent full Audits by the NCP shall take place according to epSOS Audit policy (FWA Annex II, par. 1.4).

2.1.2.44.4 e1-FLD-280 INFORMATION QUALITY-PATIENT SAFETY

2.1.2.44.4.1 e1-REQ-5297 Art. 21

The semantic transformation is performed according to the translation, mapping and transcoding performed by designated competent legal entities in the epSOS countries

- o the responsibility for the accuracy and integrity of the process is with each national designated competent legal entity for such semantic processing
- o liability for errors in the semantic mapping is a shared epSOS liability and it is managed at the level of epSOS and as part of its trust building framework.

Pilot sites are not liable for any patient safety adverse events attributed to semantic mapping.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.1.3 e1-FLD-140 Data Principle

2.1.3.1 e1-REQ-1986 Minimum and Maximum Data Sets

Synchronized with e1-REQ-5124 Minimum and Maximum Data Sets

Synchronized with e1-REQ-5128 Minimum and Maximum Data Sets

Synchronized with e1-REQ-5131 Minimum and Maximum Data Sets

Synchronized with e1-REQ-5132 Minimum and Maximum Data Sets

Related to e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Every PN MUST provide means that enable an HP IT-System to properly translate, display and process mandatory data entries within epSOS documents. Every PN SHOULD provide means that enable an HP IT-System to properly translate, display and process optional data entries within epSOS documents.

PN MAY define additional data entries within epSOS documents as long as this does not violate the defined pivot schema. PN that receive such extended documents MAY ignore all data elements not defined by epSOS.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.3.2 e1-REQ-1987 Relationships among Documents and/or Document Entries

Related to e1-REQ-4553 FR16- Univocal relation between original prescription and medicinal product dispensed

Related to e1-REQ-2111 HCER-FR09 Link HCERs

Related to e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

epSOS MUST provide means for encoding and transmitting relationships between documents and/or document entries (e. g. an eDispensation being related to a previously sent ePrescription).

Implications:

epSOS MUST make use of unique document identifiers which are stable for a long time and which are end-to-end valid/processeable among NCPs.

2.1.3.3 e1-REQ-1988 Peering Original Document

Related to e1-REQ-1961 Patient Safety

Related to e1-REQ-4549 FR12- Original prescription

Implemented by e1-REQ-2081 Implementable Original document identification

Related to e1-REQ-3900 Original document identification

Related to e1-REQ-2184 PAC FR07 Peering both original documents and translations

Synchronized with e1-REQ-5126 Peering Original Document

Synchronized with e1-REQ-5129 Peering Original Document

Synchronized with e1-REQ-5133 Peering Original Document

Related to e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Whenever original data is transcoded/translated for the purpose of cross-border document sharing, the receiver of that data MUST be enabled by epSOS to view that data without transcoding/translation, too. epSOS use case specifications MAY define default behaviors and constraints for peering original documents.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.4 e1-REQ-1703 Security Principle

Related to e1-REQ-522 Principle

All epSOS data and processes must be adequately protected. The network build among the epSOS partners should also not add any unacceptable new risk within any partner organization. Appropriate technologies and procedures must be used to ensure that data is stored processed and transmitted securely over the network build among the epSOS partners and is only disclosed to authorized parties.

Information security is generally characterized as the protection of (a) Confidentiality (information is protected from unauthorized access or unintended disclosure - only authorized users have access to the information and other system resources), (b) Integrity (information is protected from unauthorized modification), (c) Availability (resources are available, without unreasonable delay - authorized users are able to access information and the related means when they need it).

The epSOS security policy should help to ensure and enforce the above. It should also provide means of proof and essential checks, which give users trust in the given information.

2.1.4.1 e1-REQ-1708 Security Objectives: Confidentiality, Integrity, Authenticity

Related to e1-REQ-1706 Security Service Objectives.

The main objectives of information security, which follow the ISO/IEC 27001 indications, are:

Authenticity: the identity of an actor has been proven as true;

Confidentiality: information is accessible only to authorized users/[actors];

Integrity: accuracy and completeness of information and processing methods;

Availability: authorized users have access to information and associated assets when required;

Accountability/Non Repudiation (Liability): each communication and each data transaction can be tracked back to a certain originator in a traceable chain of activities.

These objectives can be further divided and applied to Actors which leads to derived security objectives. The most relevant derived security objectives for epSOS LSP are:

EntityAuthenticity: an actor is the one he/she claims to be;

Originator Authenticity: the source of data is as claimed;

Access Control: access to information is restricted to authorised actors/entities;

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Non-repudiation of origin: the data Originator cannot deny having the data;

Non-repudiation of delivery: the data Consumer cannot deny having received the data.

Taking into account the business-objectives (namely the transfer of health-care documents between two health-care organizations operating in two different MS in a way that the Consumer is able to grasp the same "clinical meaning" as expected by the Originator) and IT-objectives (as they are declared in Annex I –see [1] in the referring document list- and in WP3.1/WP3.2 -Functional Requirements-), the WP3.7 security views are:

Integrity and Confidentiality (and the derived objectives of entity authenticity, originator authenticity, and access control) are the most important security objectives as they are closely related to patient safety and to the respect of legal requirements (privacy) and massively influence the acceptance of epSOS LSP by physicians and Patients.

Accountability/Non Repudiation (liability) is important for user acceptance. Due to the trust brokering role of NCPs and the independence of physicians in deciding on their use of provided information, the liability technical aspect,in epSOS LSP, is only an issue in NCP-to-NCP communication.

Availability is important for user acceptance. Availability is a general non-functional requirements of the epSOS LSP Project as a whole.

This leads to the conclusion that integrity of medical data and certain administrative data have a high (see ref. in par. 5.1-Data classification) protection demand. The confidentiality of patient data has the same high protection demand, such as the liability (non repudiation), and the availability of epSOS LSP managed data have a moderate protection demand.

Remarks:

It must be taken into account that the confidentiality objective is influenced by the requirement that NCP has to carry out a semantic translation so, consequently, it must operate on non-encrypted clinical data and thus be under control of a natural or legal person legally authorised to process medical data. See doc#7 in the referring document list.

In order that the Consumer (HCP) is able to use the received clinical data (the data submitted to the semantic translation) for decision-making on the Patient's health, it is necessary that the received document provides the Consumer –from the integrity point of view- with the same or higher integrity assurance as the original sent document.

As there is no forecast to submit the epSOS LSP to a formal security evaluation,then the Consumer will use the received document only for decision-support.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Integrity

The original content of documents – regardless of where they come from, what they are used for or where they are shown - must always be the same and changes of the content must be consistent and traceable. From the physical perspective these requirements can be achieved by using mechanisms that protect the transmission of documents and guarantee both entities (sender and requestor/receiver) unchanged content. This protection has to be included in the basic infrastructure of communication interfaces between different systems. The technical aspects of integrity regard services which support the integration of "Security Management". These services have to respect at least two requirements. The first one is based on semantic issues which arise when the content of a document has to be translated or recoded (this issue is covered by WP3.5). The second one is important for WP3.7 because it covers tasks like prevention of altered medical information usage and protection against unauthorized access. The administrative part of integrity covers accompanying measures of "Security Management Systems".

Authenticity

When health-related data are modified or exchanged, both sides (sender and requestor/receiver) involved in such a transaction must be assured that all entities in the communication process (in terms of data transfer) are authorised to execute the designated process steps. The technical aspects such as non-repudiation, auditing of "who requested/changed what", etc. are under the conceptual responsibility of WP3.7.

Confidentiality

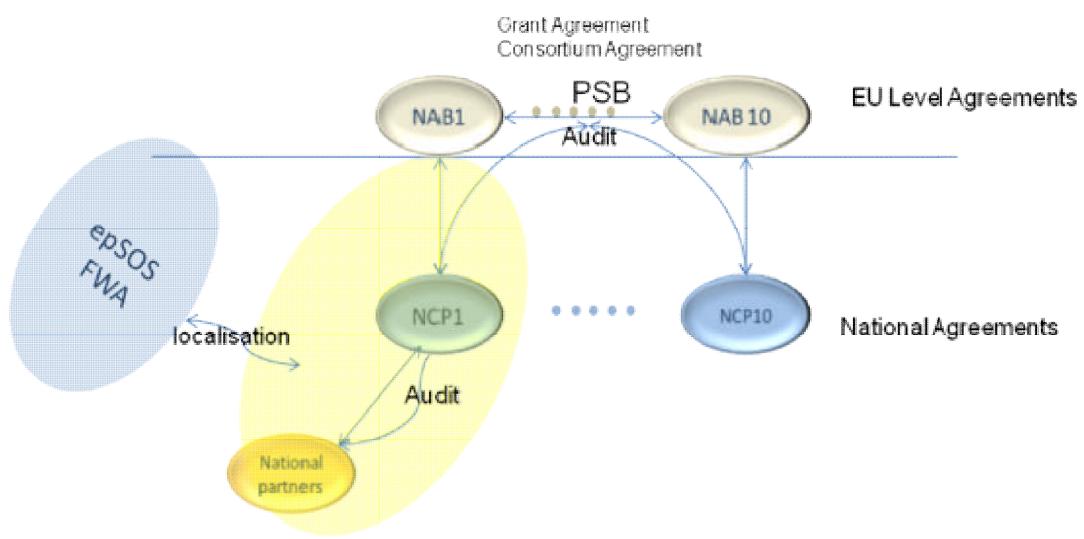
This important domain within epSOS is covered by different "Work Packages" with different approaches. From the WP3.7 point of view the physical layer of this issue can be satisfied by usage of encryption methodologies which prevent data from being humanly readable. Appropriate infrastructures and mechanisms have to be established by the MS themselves but the requirements are defined within WP3.7. Security services include the technical issues needed to achieve a high level of confidentiality. These services are not only an active support of confidentiality; they may also have passive components. An active part of these services is the separation of personal data (e.g. logon credentials or demographic data) from medical data storing (anonymization). On the other hand to achieve patients' satisfaction, a passive and proactive service which checks against "unauthorized and unwanted" access of any medical data (e.g. "emergency cases without patient consent") can be established by each MS.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.1.4.2 e1-REQ-1709 The Application of the epSOS Framework Agreement

Related to e1-REQ-63 The Application of the epSOS Framework Agreement

The epSOS Framework Agreement is intended as the common base for two levels of national agreements in order to establish the NCPs and allow the creation of NCP/HCO relationships. It is envisaged that the contracts creating the NCP in each PN will be based very closely on the FWA. The existence of national NCP contracts in each participating country which are all closely based on the FWA will ensure that collectively the NCPs can co-operate in a trusted domain to deliver their epSOS duties without the need to create direct NCP-NCP contracts.



Once the NCP is established in a PN it will in turn create contracts with HCOs and other organisations as needed, to deliver the epSOS services which will again be closely based on the terms set out in the FWA.

The legal relationships between NCPs at EU level for the pilot phase are established indirectly through their associated National Authority Beneficiaries of the epSOS Grant Agreement. The PSB is the project function established through the Consortium Agreement that ensures that NCP responsibilities are fulfilled by a transparent and independent audit system to be also approved by the PSB.

The epSOS legal approach, described in D2.1.1, envisages that the operation of pilots will become possible through use case specific safeguards for the protection of patients rights, including those for processing of health information with proper balancing of patients' and public health interests that should be guaranteed by all pilot sites. Safeguards are primarily measures to be taken during the pilot operation not only by the NCPs but also by the PoC that the mobile

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

citizen will come in contact with.

Given these expectations we foresee broadly two sets of requirements for PoC: (i) to put in place appropriate measures (processes and procedures, including security measures and safeguards) and (ii) to maintain records and reports demonstrating compliance to such measures, to be used for traceability and audit purposes.

The epSOS Security and the Audit policy has been adopted by the PSB and annexed to this FWA under Annex III.

WP3.8. has furthermore elaborated guidance on the NCP security policy and audit.

At the organizational level, these requirements should be considered in a generic way, without imposing specific procedures to the MS, but still setting the criteria for mutual recognition and acceptance.

The FWA therefore constitutes a contractual agreement between NCP-PSB which is monitored through independent audit of conformance to this FWA. The PSB role as primary arbitrator between NCPs (see section 2.2) allows the PSB to act as mediator but also enables the PSB to adopt epSOS performance standards and allow or control variations to FWA.

The collectivity of all the relationships between the NABs at international level as well as the NABs- NCPs and the NCP-HCO nationally will together form the legal basis for the delivery of the epSOS pilot services.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.1.4.3 e1-REQ-1717 epSOS processes

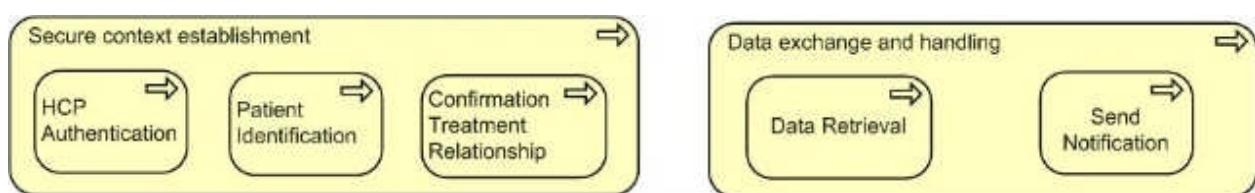
The scope of this sub-chapter is to support the identification of services. One of the powerful aspects of services oriented approach in respect of messaging or transaction approach is the capacity to design generic services, reusable in different scenarios versus the definition of messages tightly coupled with the specific integration context.

In epSOS, the two different contexts (ePrescription and Patient Summary) share the same basic business activities into 2 main steps:

Secure context establishment

Data Exchange and Handling

The epSOS core business processes can therefore be represented as such:



2.1.4.4 e1-REQ-4615 REQ 3.3.31 Exception Handling

Related to e1-REQ-1994 Robustness

EpSOS must be secure even if a failure arises. The involved actors should stay in a well-defined state with a well-defined fault handling.

Exceptional events MUST be reported among system components in a way that allows the systems that are affected by the failure to process the respective message in a way that:

an appropriate reaction can be taken

further dependent failures are prevented

as few system components as possible are affected

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.4.5 e1-REQ-1829 Use existing infrastructure of the member states for certificates

There is common agreement that epSOS will minimize centralized infrastructure, hence not implement its own certificate authority.

2.1.4.6 e1-REQ-1993 Scalability wrt Availability, Performance and Throughput

Related to e1-REQ-1996 Continuous Improvement

Related to e1-REQ-1991 Extensibility of the Use Cases

Related to e1-REQ-1992 Use of Standards

Related to e1-REQ-4590 REQ 3.3.5 Synchronous Communication

epSOS services SHOULD be adaptable to changing requirements on availability, performance and throughput. NCP reliability and performance SHOULD not decrease if the number of documents shared through this NCP increases. The epSOS architecture and service design SHOULD not put restrictions on service levels to be defined between epSOS users and epSOS service providers.

Implications:

epSOS NCPs SHOULD be stateless in order to allow for implementing horizontal scalability and node/service redundancy by standard means.

2.1.4.7 e1-REQ-1994 Robustness

Related to e1-REQ-4615 REQ 3.3.31 Exception Handling

Related to e1-REQ-1995 Recoverability

epSOS services SHOULD be robust in a way that they enable epSOS users to proceed (maybe with limited information) with their current medical tasks even in cases of unexpected behavior of human users and/or communicating components.

Implications:

System behavior SHOULD be aligned with a typical user's conceptual model of epSOS design and operations even in cases of partial system failures.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.4.8 e1-REQ-1995 Recoverability

Related to e1-REQ-1994 Robustness

Even in cases of failures of epSOS components there MUST NOT be any loss or corruption of medical data. After medical data is taken over by an NCP, this NCP takes full responsibility for the further processing and transmission of that data.

Implications:

epSOS services SHOULD be stateless whenever possible. epSOS service calls SHOULD behave like transactions to the user.

2.1.5 e1-FLD-141 Business processes

2.1.5.1 e1-REQ-1966 Request for Medical Data

Related to e1-REQ-1991 Extensibility of the Use Cases

epSOS MUST provide functionalities to HP-B that allow him to request medical data of patient-A.

HP-B is acting from within country B. The request for patient-A data is processed by country A. The request contents, the expected result sets and the expected behavior of the involved actors MUST be defined as part of each epSOS use case specification that makes use of this functionality. The implementation of this functionality is mandatory for all countries A and B. The epSOS scope only covers the mediation of the request between national gateways (NCPs).

Implication:

epSOS MUST define business processes and services for forwarding requests for data from country B to country A.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.5.2 e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1991 Extensibility of the Use Cases

Related to e1-REQ-1986 Minimum and Maximum Data Sets

Related to e1-REQ-1988 Peering Original Document

Related to e1-REQ-1987 Relationships among Documents and/or Document Entries

Related to e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-1984 Data Origin and Data Authenticity

Related to e1-REQ-1985 Patient Data Assignment

epSOS MUST provide functionalities to provide medical data of patient-A to HP-B. The provisioning of medical data by country A MUST only be performed upon request by HP-B (see “Request for Medical Data”).

The data transmitted and the expected behavior of the involved actors MUST be defined as part of each epSOS use case specification that makes use of this functionality. The implementation of this functionality is mandatory for all countries A and B. The epSOS scope only covers the mediation of the provided data between national gateways (NCPs).

Implication:

epSOS MUST define business processes and services for transmitting medical data from country A to country B.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.5.3 e1-REQ-1969 Provisioning of Medical Data by Country B

Related to e1-REQ-1967 Country-A as Primary Source

Related to e1-REQ-1991 Extensibility of the Use Cases

Related to e1-REQ-1986 Minimum and Maximum Data Sets

Related to e1-REQ-1988 Peering Original Document

Related to e1-REQ-1987 Relationships among Documents and/or Document Entries

Related to e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-1970 Consent Registration

Related to e1-REQ-1984 Data Origin and Data Authenticity

Related to e1-REQ-2100 HCER-FR02 Country A is informed of treatment event in country B

Related to e1-REQ-1985 Patient Data Assignment

epSOS MUST provide functionalities to HP-B that allow him to transmit medical data about patient-A to country A.

The data transmitted, valid responses from country-A and the expected behavior of the involved actors MUST be defined as part of each epSOS use case specification that makes use of this functionality. The request contents, the expected result sets and the expected behavior of the involved actors MUST be defined as part of each epSOS use case specification. The implementation of this functionality is mandatory for all countries B (>epSOS Extension). A country A that does not implement this functionality MUST reject respective requests from HP-B. It is country-B responsibility to define alternative means for transmitting the respective information to country-A (e. g. printing it on paper and handing it to the patient). The epSOS scope only covers the mediation of the provided data between national gateways (NCPs).

Implication:

epSOS MUST define business processes and services for transmitting medical data from country B to country A.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.5.4 e1-REQ-4441 Process “HP accessing health data of a patient” (with given consent)

Related to e1-REQ-4443 REQ 3.6.35 Access to patient's health data

Related to e1-REQ-4444 REQ 3.6.36 Transmitted attributes in health data access attempts

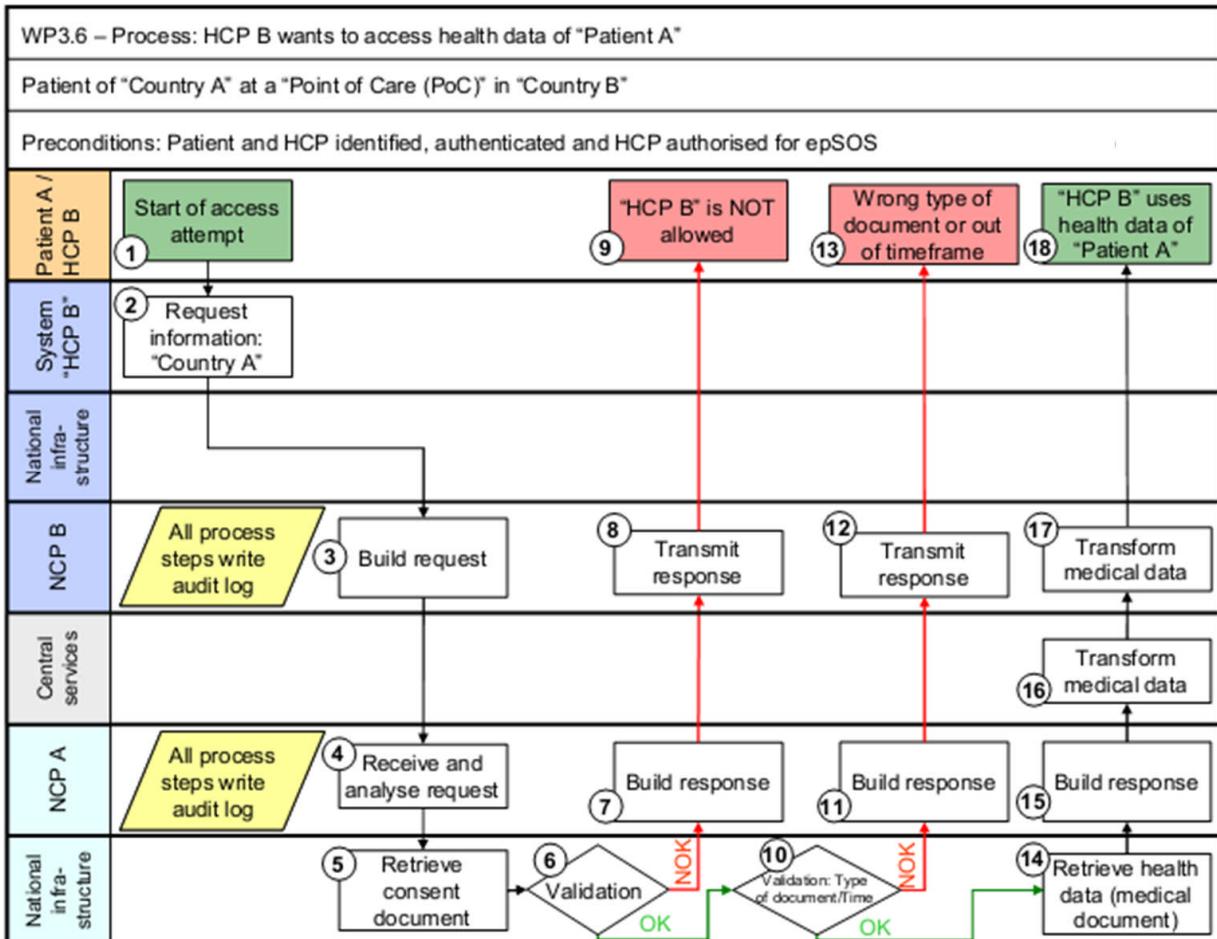
All health data of a patient that can be accessed by the means of epSOS LSP are managed within the existing national infrastructures. It is assumed that all data of a patient is indexed with a patient identifier ("index key") that is issued and managed by the national infrastructure. If a patient has data within multiple national infrastructures, these might be indexed by different patient identifiers.

In order to access data or in order to assign new data to a patient, the respective identifier of the patient that is used as an index key within the national infrastructure must be known by NCP A which initiates the respective data access operation. If data is accessed from another country (Country B) the NCP of this country must be aware of a patient identifier that allows NCP A the unique mapping of this identifier onto the data indexing identifier.

This recommended process describes the case in which a HP at PoC in Country B wants to access the health data of a patient of Country A. A patient is situated at PoC and is already identified and authenticated and a HP is also already identified, authenticated and authorised for epSOS LSP.

An access attempt to medical information of a patient is caused by three conditions: Country B is allowed for access to health data, accessed data are of allowed type and timeframe for consent is valid. Fulfilling these conditions, the national infrastructure in Country A retrieves health data from national registry and sends requested health data to a HP in Country B (for details, see pictures and descriptions below).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



1. HP and patient are situated at the PoC in Country B and HP wants to access medical information of patient – start of access attempt. The first step in this process includes the revalidation of the authorization of the HP for epSOS LSP.
2. HP from his local system requests NCP B for medical information from Country A.
3. NCP B receives the request from HP system and writes an audit log. Then NCP B builds the request (or maps it to Country A) for NCP A for medical information and writes an audit log.
4. NCP A receives and analyses the request from NCP B and writes an audit log. The analysis includes the completeness and the roles.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

5. Then NCP A confirms to NCP B the reception of the request and writes an audit log. NCP B receives the confirmation and writes to audit log. NCP A sends a request for medical information to national infrastructure in Country A and writes an audit log.

6. National Directory in Country A retrieves the consent document of patient.

7. The national infrastructure in Country A checks the status of patient consent for Country B

a. The national infrastructure in Country A checks the status of patient consent for Country B

i. One of the following results is returned: patient consent for Country B is NO - Country B is not allowed - (continue on step 8) or patient consent for Country B is YES - Country B is allowed - (continue on step 11). If patient restricted some documents or selected only specific HPs the document will not be sent to country B. This depends on national law of Country A and possible restrictions by a patient.

b. Checking of the role of epSOS LSP actors

i. Not all roles of epSOS LSP actors have access to the health data (depending on national laws of MS)

8. NCP A receives from national infrastructure in Country A the result NO of consent for Country B and writes an audit log. NCP A builds the response (or maps it to Country B) to NCP B on result of consent and writes an audit log.

9. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HP and writes an audit log.

10. HP's access to medical information of patient is refused, because Country B is not allowed to access this information – process is finished.

11. Additional Validation will be done:

a. The national infrastructure in Country A checks the type of requested document (type of medical information). One of the following results is returned: patient consent for Country B is NO for this type of document (continue on step 12) or patient consent for Country B is YES for this type of document (continue on step 15)

b. The national infrastructure in Country A checks the timeframe for consent (status YES) of the requested medical information. One of the following results is returned: the request is not within consented timeframe (continue on step 16) or the request is within consented timeframe (continue on step 15).

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

12. NCP A receives from national infrastructure in Country A the result NO of consent for type of document and writes an audit log. NCP A builds the response (or maps it to Country B) to NCP B on result of consent and writes an audit log.

13. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HP and writes an audit log.

14. HP's access to the requested type of medical information of patient is refused – process is finished.

15. The national infrastructure in Country A retrieves the medical document (medical information) from national repository and sends it to NCP A.

16. NCP A receives from national infrastructure in Country A the medical document of patient and writes an audit log. NCP A builds the response (or maps it to Country B) to NCP B on medical document and writes an audit log.

17. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HP and writes an audit log.

18. HP uses the medical document of patient of Country A at PoC in Country B – the process is finished.

2.1.5.5 e1-REQ-4445 Process “HP accessing health data of patient” (emergency case)

Related to e1-REQ-4446 REQ 3.6.37 Processes for emergency cases

Related to e1-REQ-4447 REQ 3.6.38 County A decides in emergency cases

The main differences to the above described process is that the HP identifies (if patient is responsive and not unconscious) the patient either with an e-ID, other identifiers or with demographic data (whatever is available) and the consent in Country A is NOT checked if the "PURPOSE-OF-USE" attribute is set to "EMERGENCY" in the request of health data.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.1.5.6 e1-REQ-1970 Consent Registration

Related to e1-REQ-2210 L-DP-06 Patient Consent accounting for purpose and manner of data processing

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Related to e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

epSOS MUST define functionalities that allow the Patient – while at a physician in country-B – to give an informed consent on epSOS and to register this consent with country-A.

The registration of the consent MAY as well be done by the HP to whom the patient gave the consent. The implementation of this functionality is optional for all countries A and B. A country A that does not implement this functionality MUST reject respective requests from HP-B. If a country-A does not implement this functionality, country-A SHOULD define alternative means for registering a consent with country-A (e. g. printing and signing it on paper and then sending it by Fax or eMail to the country-A epSOS NCP service desk).

Implication:

epSOS MUST define business processes and services for transmitting consent forms from country B to country A.

2.1.5.7 e1-REQ-1972 Patient Access

Related to e1-REQ-1967 Country-A as Primary Source

Related to e1-REQ-2178 PAC FR01 Patient Access basic requirement

epSOS MUST define functionalities that allow the Patient to access own medical information available at her country of affiliation and/or get her medical information translated into any epSOS PN language. Even though these functionalities are defined by epSOS, they MUST be specified, implemented and operated by each country-A based on that countries legal framework and technical abilities.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.1.5.8 e1-REQ-1973 Patient Identification

Synchronized with e1-REQ-3868 Patient Identification

Synchronized with e1-REQ-4540 Patient Identification

Synchronized with e1-REQ-4673 Patient Identification

Synchronized with e1-REQ-5077 Patient Identification

Synchronized with e1-REQ-5078 Patient Identification

Synchronized with e1-REQ-5079 Patient Identification

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

The intended recipient of medical data MUST identify the patient with sufficient accuracy. Medical data MUST only be disclosed after the patient was identified with sufficient accuracy.

Technical means for patient identification MUST NOT use or disclose medical data about this patient. Patient identifiers SHOULD NOT technically enable any unlawful linkage of the patient's medical data to other sanctioned personal data beyond any legitimate purpose from other domains. If technical means for identity protection (e.g. pseudonymization) are used, these MUST NOT disqualify the responsible parties to lawfully provide the patient access to his/her data. The original identification of the patient MUST NOT rely on the existence of electronic identifiers (eIDs). epsos use cases MAY define further constraints on the accuracy and means of patient identification for that specific use case (e.g. identification by name considered as insufficient for the 112 use case).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.1.5.9 e1-REQ-4614 Process secure context establishment between 2 NCPs

Related to e1-REQ-4591 REQ 3.3.6 Secure Context Establishment

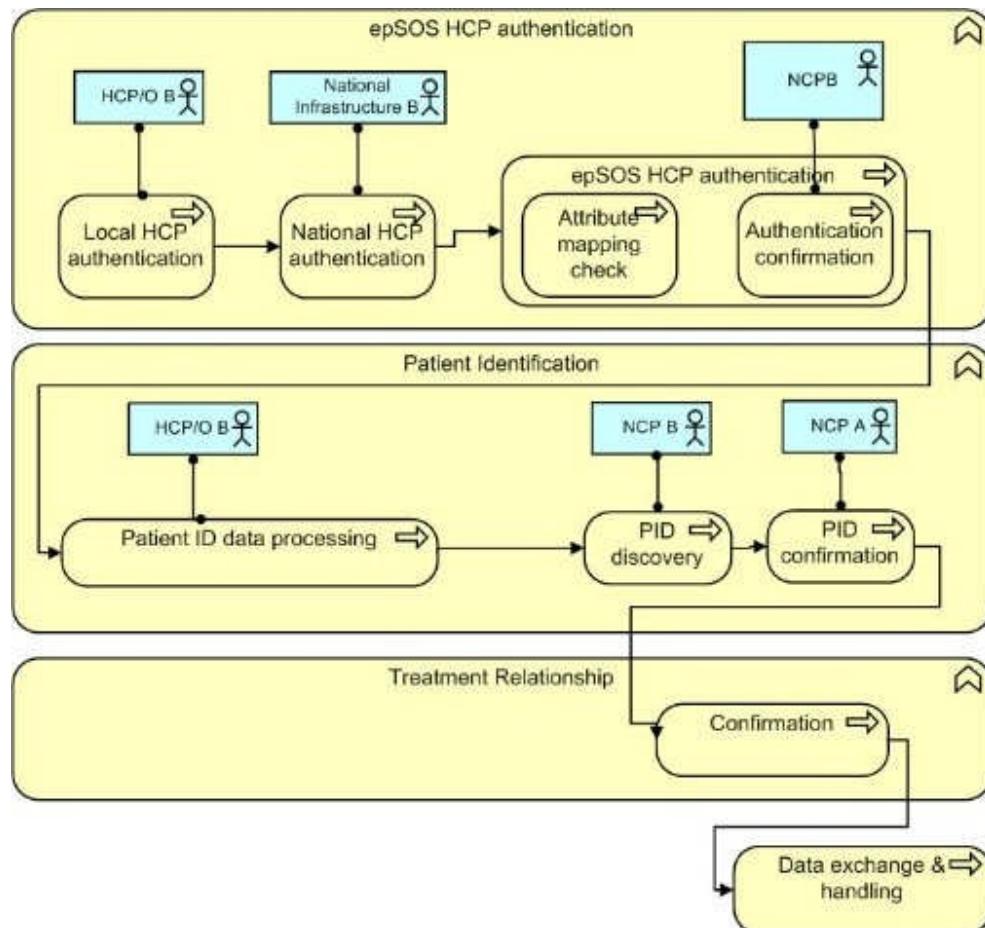


Figure: Secure Context Establishment

Basically:

Step 1: a HP is identified and is authorized to access the epSOS System,

Step 2: A Patient Identification process follows,

Step 3: The Confirmation of the Treatment Relationship is established between the patient and the HP(O)

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The **Secure Context Establishment** supports the separation of basic security concerns from the business transactions. The later is achieved by defining a security context that the business transactions can rely on. Before an epSOS transaction is carried out on business level, a chain of trust relationships between the involved actors has to be established. This chain of trust is based on (mutual) authentication. The above figure shows the necessary steps.

The HP authentication allows for the health profesional at PoC-B its authentication in country B. For the authentication of the health profesional at PoC-B - who issues the request - and for the authorisation of that health profesional at PoC-B by the patient - who is the owner of the requested medical data object - country A has to trust the processes of country B.

The Patient identification between country A and country B in order to allow for ID mapping in such a way that ID domain, on one hand, and medical data domain, on the other hand, can be strictly separated. The process starts routing calls to NCP-A. Patient ID data is entered by health profesional at PoC-B of country B and information regarding patient's country is given. Based on that mutual trust the patient identification and authentication (as far as required by country A) is done, initiated by the health profesional at PoC-B of country B but controlled by the NCP-A.

The Treatment Relationship Confirmation is established between the health profesional at PoC-B and the patient. A treatment relationship is validated when the health profesional at PoC-B checks the box provided by his regular interface.

2.1.5.10 e1-REQ-4986 Semantic Content Workflow

Related to e1-REQ-1950 Taxonomy for the epSOS pivot format central function

HP-B sees Patient-A who has Country A as country of affiliation and requests from NCP B the patient's information.

Transactions to retrieve Patient-A files are initiated between NCP B and NCP A.

A document A containing among other information, Patient-A pathologies, created by HP-A is sent to NCP A. Patient-A pathologies are coded with Code A /displayName A (4-digits ICD-10 code, A language). *Note: the same process is valid for regional 5-digits ICD-10 codes.*

NCP A transcodes Code A to epSOS Code (Code E) by removing the fourth digit from Code A.

epSOS English Display Name (displayName E) is retrieved from the epSOS MTC, and both Code E and displayName E are entered into a newly created Document E. (Pivot Document in Country A) Code A and DisplayName A are kept within the same document in their original form.

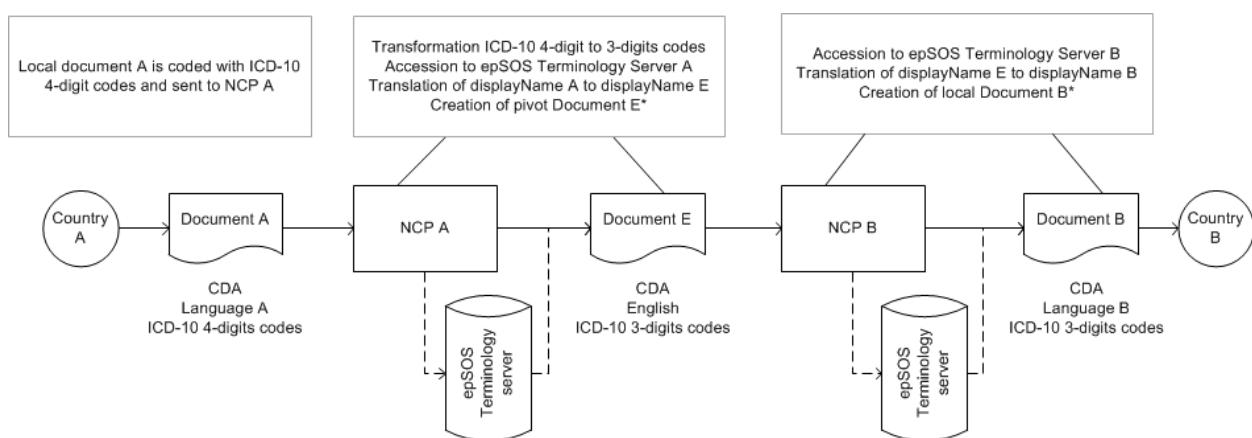
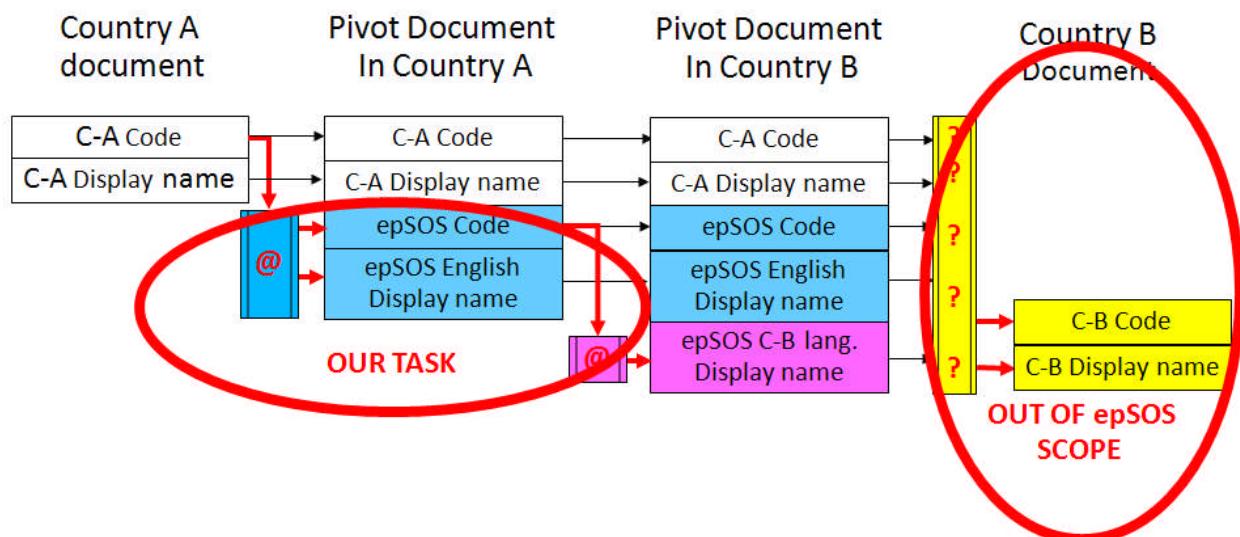
	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

After retrieving Document E, NCP B, using Code E, retrieves the displayName in B language from the epSOS MTC.

NCP B creates a Document B (Pivot Document in Country B), places the displayName B into it and sends the document B to the HP-B.

HP-B can now see Code B and displayName B, in language B. He can also see the initial Code A and displayName A which were kept into the document for additional information.

The following illustrations depict the process described above:



 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.1.6 e1-FLD-142 Information Dimension

2.1.6.1 e1-REQ-1669 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-5142 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-5143 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-5144 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-5145 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-5146 About HP Prescriber Identification in the ePrescription

Variable	Definitions	MS: Minimum Max: maximum	Comments	Example
Given Name	The Name of the Prescriber	MS	This field can contain more than one element	Marta
Family name/surname	The surname/s of the Prescriber	MS	This field can contain more than one element	Español Smith
HP Id number	The identification of the person as HP	MS		12345
Profession		MS		Physician
Specialist		Max		Dermatologist
Prescriber Facility Address:	The place (complete address) where the prescriber made the prescription		This is not a field but a block of information made up of the following fields. This might not be in the dataset but	e.g., Los Bermejales Health Care Centre. Alemania St. Seville, 41018. Spain

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

			this information needs to be available for the process traceability (FR20)	
Name of the Facility		Max		For instance, the name of the building: Los Berrmejales
Street Address		Max		Alemania Street
City		Max		Seville
State or Province		Max		Seville
Zip or Postal Code		Max		41018
Telephone		Max		+34 954123123
Contact email of the centre or of the prescriber		Max		losbermejaleshealthcentre@xxx.es
Country	The country where the prescription was made	MS	The dispenser needs to know the country where he is consulting the information from	Spain
Prescriber Organization:			This is not a field but a block of information made up of the following fields. This might not be in the dataset but this information needs to be	

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3	
	Version:	1.0
D5.2.3	Date:	31/01/2013

			available for the process traceability (FR20)	
Organization Name		Max		e.g. Andalusia Health Service
Organization Identifier		Max	This field can be numbers and/or letters	123458xfs

2.1.6.2 e1-REQ-4974 NCP-Req#3.7.18 (Minimum Content of Accounting Logs)

Related to e1-REQ-4452 REQ 3.6.12 Audit trail definitions

the logs SHOULD contain:

- the user ID of the accessing User
- the role the User is exercising
- the organisation of the accessing User (at least in those cases where an individual accesses information on behalf of more than one organisation);
- the unique Patient ID
- the function performed by the accessing User
- the NCP-id of the Originator/Target
- a time stamp including time zone used

2.1.6.3 e1-REQ-4452 REQ 3.6.12 Audit trail definitions

Related to e1-REQ-4974 NCP-Req#3.7.18 (Minimum Content of Accounting Logs)

Definition must be done from national site under national law.

The general structure of audit log includes (not restricted to):

User IDs;

Dates, times, and details of key events, e.g. log-on and log-off;

Terminal identity (either terminal-ID in a hospital or IP number) or location if possible;

Records of successful and rejected system access attempts;

Records of successful and rejected data and other resource access attempts;

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Changes to system configuration;

Use of privileges;

Use of system utilities and applications;

Files accessed and the kind of access;

Network addresses and protocols;

Alarms raised by the access control system;

Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

The audit logs may contain sensitive personal data. Appropriate privacy, integrity and availability protection measures should be taken. A standard option in protecting audits logs is performing their on-line back up on a log server. In this case, the audit logs are stored at two places, at the servers of their creation and at the dedicated log server.

Following the required items of audit log format for both cases of identification and authentication of epSOS LSP entities are given.

Identification and authentication of a HP:

- The audit log written by NCP B should contain these items:
 - Time reference
 - ID of HP and provider of ID
 - Authorisation request
 - Attributes of HP (role, specialisation) and provider of attributes

Identification and authentication of a patient:

This process supposes the successful identification, authentication and authorisation of HP for epSOS LSP.

- The audit log written by NCP should contain these items:
 - Time reference
 - ID of patient and provider of ID
 - Other country NCP

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

- Type and/or transaction data (identification data, confirmation of transfer, result of identification, etc.)
- Inbound NCP and outbound NCP
- ID of epSOS LSP session

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Following the required items of audit log are given. The audit log written by NCP should contain these items:

- Time reference
- ID of patient and HP
- Other country NCP
- Type and/or transaction data (patient consent for Country B, result if validation allowed, consent update, confirmation of transfer, etc.)
- Inbound NCP and outbound NCP
- ID of epSOS LSP session

2.1.6.4 e1-REQ-4444 REQ 3.6.36 Transmitted attributes in health data access attempts

Related to e1-REQ-4446 REQ 3.6.37 Processes for emergency cases

Related to e1-REQ-4441 Process “HP accessing health data of a patient” (with given consent)

Based on the analysis of the PN-specific operation of the National Security Policies, epSOS must be able to communicate not only identity information but additionally a set of assigned attributes. A set of minimal attributes is proposed to be designed as follows:

Attribute	Mandatory	Constraints
ROLE	YES	medical doctors (general medical practitioners, special medical practitioner), nursing professionals, midwifery specialists, pharmacists, medical data administrators
SPECIALTY	NO	GP, urologist, cardiologist, etc.
COUNTRY-OF-CARE	YES	Country where health service is provided
ON-BEHALF-OF	NO	This attribute supports the legitimate delegation of rights to appointed medical assistance personnel. In many Member States, a HP may delegate certain tasks to assisting personnel acting on his behalf with a subset of his access rights: e. g. nurse acting on behalf of a physician.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

TYPE-OF-ORGANISATION	YES	hospital, physicians practice, emergency car, etc.
PURPOSE-OF-USE	YES	standard, emergency, etc.

2.1.6.5 e1-REQ-4984 Master Value Set Catalogue

Related to e1-REQ-4985 Master Translation/Transcoding Catalogue

The **MVC** (Master Value set Catalogue) is a data structure containing all the value sets selected in epSOS. The value sets should represent the codes needed for a PN to being able to send the information needed in the three pivot documents: ePrescription, eDispensation and Patient Summary.

Every value set has a name, a universally unique identifier OID, version, date and a reference to the parent Code System identifier. Each concept is represented by a code and english display name.

2.1.6.5.1 e1-TXT-777 Note

Please note that **the value set OID is used for management purposes only and not in the syntax of the pivot documents.**

Most of the OIDs for the code systems are the official ones from the respective SDOs. In cases where an SDO does not have an OID for a Code System, an OID was assigned in the epSOS context.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.1.6.6 e1-REQ-4985 Master Translation/Transcoding Catalogue

Related to e1-REQ-4984 Master Value Set Catalogue

The **MTC** (Master Translation/Transcoding Catalogue) is the set of :

(a subset of the) MVC value sets translated by the PN Terminology Responsibles

If any, the mapping tables between PN Value Sets and the epSOS ones needed for managing the local codes transcoding/mappings

The MTC is a copy of the MVC but without the technical value sets which should not be translated.

2.1.7 e1-FLD-191 High level architecture

2.1.7.1 e1-TXT-772 Note

The epSOS architecture as presented as follows is abstracted from the complexity-characteristic-platform of underlying systems (loose coupling principle), thereby giving guidelines for a pilot implementation of an epSOS NCP. The specific technical implementation of a service should be hidden for the consumer. The components of an epSOS National Contact Point (NCP) can be viewed like a logical “wrapper” of the different National Infrastructures.

2.1.7.2 e1-REQ-1953 epSOS Domains

The following figure illustrates the different domains of epSOS. Domains categorize those capabilities:

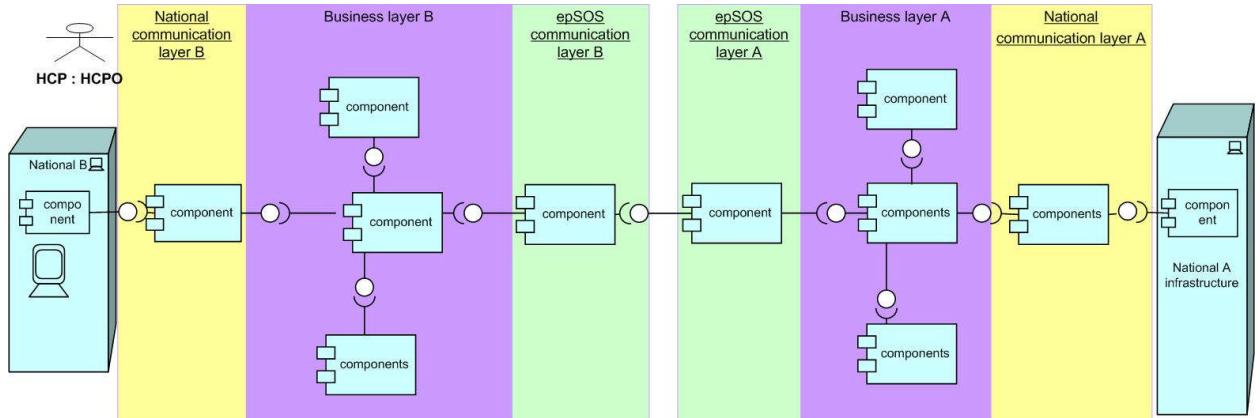
National infrastructure (National Infrastructure of HP and HPO)

National communication layer

Business layer

epSOS communication layer

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013



This does imply technically:

epSOS communication layer includes components with common Interfaces that MUST be considered as "normative" with Web services that use open, XML-based standards and transport protocols to exchange data between Gateways.

Business Layer does implement components specified in a Platform Independent model for this document. This layer includes all components and their specific interfaces, to resolve specific business functions of epSOS. The components in this layer do not directly communicate to the national infrastructure or exchange messages with other NCPs.

National communication layer Infrastructure interfaces are strictly related to national infrastructure and specified only at functional level, hence they are described as abstracted from the application type (national responsibility). Only the Interfaces of the components can be described, but the implementation is more a national concern because of the heterogeneity of national infrastructure.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.7.3 e1-REQ-4948 Common Components Composite Structure

The following common components have been identified by the technical core team:

InboundProtocolTerminator

OutboundProtocolTerminator

SecurityManager

TransformationManager

TerminologyServiceAccessManager

WorkflowManager

AuditTrailWriter

AuditRepository

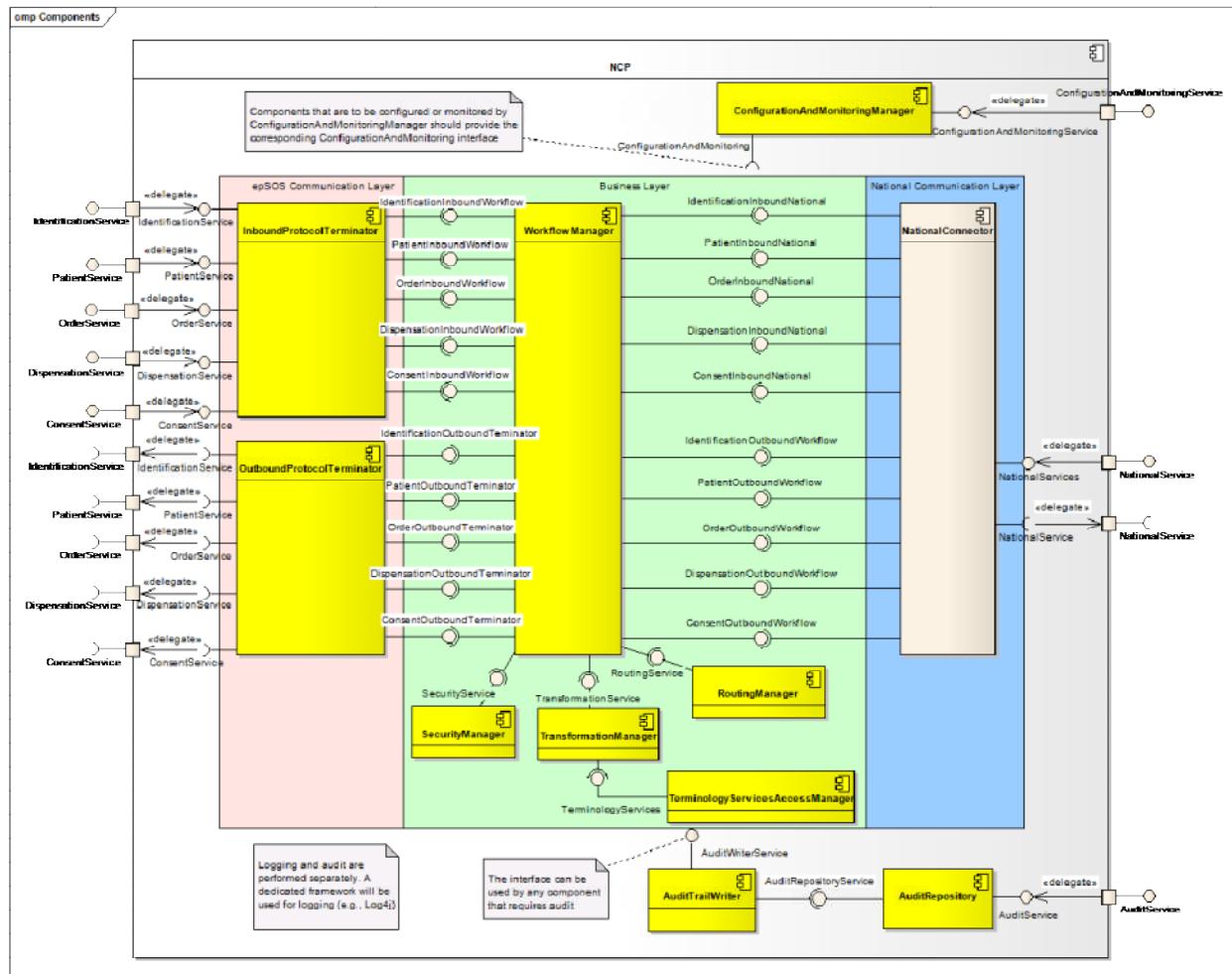
RoutingManager

ConfigurationAndMonitoringManager

NationalConnector

The following picture illustrated the link between services and technical components.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013



Components that are not common but part of the NCP gateway are grouped in the NationalConnector. The basic concepts of the architecture are derived by the logical sectioning of the NCP gateway into three vertical layers (domains). The workflow manager is the component which is responsible for managing communication between the layers .

2.1.7.3.1 e1-REQ-4949 InboundProtocolTerminator

The *InboundProtocolTerminator* plays the role of epSOS web services provider and is responsible for providing SOAP web services. It implements the endpoint of the epSOS services and performs verification of WS-Security SAML tokens as well as deserialization of SOAP message into objects. The resulting objects are passed to the *WorkflowManager* who passes them further to the corresponding components. When the *WorkflowManager* returns the

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

resulting object, the *InboundProtocolTerminator* serializes the object in to a SOAP message and passes it as a SOAP response to the corresponding NCP endpoint address.

2.1.7.3.2 e1-REQ-4950 OutboundProtocolTerminator

The *OutboundProtocolTerminator* plays the role of a Web Service consumer. It serializes message objects in a SOAP request, adds corresponding WS-Security tokens and routes it to the NCP endpoint address of the country of affiliation of the patient. When the response arrives, it performs the deserialization of the SOAP response into a message object and transfers the object to the *WorkflowManager*.

2.1.7.3.3 e1-REQ-4951 WorkflowManager

The *WorkflowManager* is called from the *InboundProtocolTerminator* as well as from the *NationalConnector*. This component realizes a Process Manager pattern. It is the entry point into the business layer of the NCP. Therefore this component is the first to be called after a message is received and serialized. The *WorkflowManager* acts as orchestrator and realize the chain of operations call. The operations are exposed by interfaces of others components of business layer and, at the end, the result will be passed to the *OutboundProtocolTerminator* or to the National Connector.

2.1.7.3.4 e1-REQ-4952 SecurityManager

The *SecurityManager* is used for certificate validation and XML-Signature creation and validation. It is mandatory that the security manager has a list of all trusted certificates to check whether the given certificate is member of the circle of trust. The certificate validation includes the mathematical check, the check of the validity in time and the OCSP call.

2.1.7.3.5 e1-REQ-4953 TransformationManager

Related to e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

This component generates an epSOS Pivot document by translating and/or transcoding (if necessary) the original data compliant to epSOS CDA syntax from the national language and possibly from the national code system(s) in the document creator country (in most cases Country A) to the epSOS Reference Terminology. From a functional point of view the translation and transcoding are the same operation for the Transformation Manager. In fact, translation/transcoding is facilitated by calling the *TerminologyServicesAccessManager*. Moreover, it creates an epSOS unstructured CDA by embedding the original data from document creator presented in the pdf format.

2.1.7.3.6 e1-TXT-771 Note

Note: the assumption is made that the original data is already presented in a pdf format.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.1.7.3.7 e1-REQ-4954 TerminologyServicesAccessManager

This component is called by *TransformationManager*. The component is responsible for translating a given concept designation into the requested target language as well as transcoding a given “local” coded concept into the appropriate epSOS coded concept using the information present in the Terminology Repository. The Terminology Repository is a database representation of the epSOS Reference Terminology.

It must be noted that the epSOS Reference Terminology has as a starting point the epSOS Master Value Sets Catalogue (MVC), which in turn is the basis for the epSOS Master Value Sets Translation/Transcoding Catalogue (MTC) (see D3.5.2 for further details). The mapping activity from the “local” coded concept to the epSOS Value Sets present in the epSOS MVC is out of scope of epSOS and it is the responsibility of the National Linguistic Competence Centers from each participating nation. This mapping is compiled in the epSOS MTC. The maintenance of the MTC and its relationship with the MVC are out of scope of the common components design.

2.1.7.3.8 e1-REQ-4955 RoutingManager

Before any message can be sent by the NCP (in the role of country B), information for the correct routing to the corresponding NCP (in the role of country A) must be resolved. The outcome of the *RoutingManager* is a URL of the corresponding NCP.

2.1.7.3.9 e1-REQ-4956 ConfigurationAndMonitoringManager

The *ConfigurationAndMonitoringManager* provides a monitoring console that is used for managing configurations of the nation-specific components as well as monitoring their status. As one of its subcomponents, ConfigurationAndMonitoringManager should include an Abuse Detection System. This subcomponent should be responsible for analyzing the audit trail and, based on a configurable rule set, prevent possible abuses (such as excessive requests issued from a HP or a patient queried from more than one country at a time).

2.1.7.3.10 e1-REQ-4957 NationalConnector

The *NationalConnector* is not a common component, but a collection of adapters to the national protocols and data formats. The *NationalConnector* makes use of a common exposed API as required by the *WorkflowManager* as well as exposes a common API to the *WorkflowManager* itself. The interface to the national infrastructure, however, is country-specific with no restrictions imposed on it.

2.1.7.3.11 e1-REQ-4959 AuditTrailWriter

This component addresses the need to audit every transaction in epSOS. National requirements for an extended auditing must be realized in the *NationalConnector* or the national infrastructure.

2.1.7.3.11.1 e1-TXT-770 Note

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Note, that it should be differentiated between logging and audit. Audit captures business-level events (e.g., request for PS) while logging occurs on a lower level and is responsible for capturing application-level events

2.1.7.3.12 e1-REQ-4958 AuditRepository

This component is responsible for storing audit trail that is captured by *AuditTrailWriter* component. Additionally this component exposes an interface that is used by the national infrastructure to selectively querying fragments of the audit trail.

2.2 e1-FLD-32 Logical Perspective

2.2.1 e1-FLD-145 Security architecture

2.2.1.1 e1-REQ-1789 Definition of elements and actors relevant for security issues

In this section the elements (data classes) and actors in the epSOS LSP are considered from a security point of view.

2.2.1.1.1 e1-REQ-1790 Data classification

A generalized data classes are introduced together with their protection requirements. Each element in the epSOS LSP belongs to one of these data classes.

The following data classification is considered in epSOS LSP:

Healthcare-related Data: Healthcare Data of a patient e-prescription or patient summary used for the medical treatment of a patient. According to the Directive 95/46/EC the processing of medical data has to satisfy higher privacy requirements since they belong to the special categories of data (Article 8 Directive 95/46/EC). Healthcare related data contain also:

data about the patient's consent;

log data which provide information about the access to healthcare related data in epSOS LSP.

Critical Meta Data: Data needed to control the exchange of healthcare related data between NCPs and between NCPs and PoCs, respectively. Critical Meta Data include authentication, identification and administrative data to clearly identify patients, PoCs and HCPs,

Non-critical personal data: Personal data which do not belong to the special categories of data according to Article 8 Directive 95/46/EC and do not belong to the critical meta data.

Administrative Data: They do not contain any personal data. They are used for the administration or configuration of technical components.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

The data classes differ in the damage that could occur if the confidentiality, integrity, or availability are lost.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

Impact dependent on threat and data class

Threat	Healthcare-related Data	Critical Meta Data	Non-critical personal data	Administrative Data
Violations of laws, regulations, or contracts	Can have substantial consequences, for example violates national privacy laws or professional secrecy laws	Can have substantial consequences, for example violates national privacy laws or professional secrecy laws	Can have substantial consequences, for example national privacy laws	Have minor consequences
Impairment of privacy	Processing could have a seriously adverse effect on the social standing of the persons.	Processing could have a seriously adverse effect on the social standing of the persons.	Processing could have an adverse effect on the social standing of the persons.	No damage on privacy
Physical injury	Serious injury to an individual is possible. There is a danger to life and limb (e.g. a medical treatment based on modified and false health-care data may have serious consequences on the state of health of a person).	Serious injury to an individual is possible.	Does not appear possible.	Does not appear possible.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Negative internal or external effects	Considerable impairment of the reputation /trustworthiness can be expected.	Considerable impairment of the reputation / trustworthiness can be expected.	Only minimal impairment or only internal impairment of the reputation / trustworthiness is expected.	Only minimal impairment or only internal impairment of the reputation / trustworthiness of the organisation is expected.
Financial impacts are not considered here				

The impacts of the damages on the confidentiality, integrity, availability, authenticity and non-repudiation of the data in data classes are qualified in terms of high, moderate, and low impact according to [FIPS 199]. The level for availability is set to low, since there are existing alternative processes (patients are treated already today), so that a medical treatment is also guaranteed without the epSOS LSP data.

Impacts level

Data class	Confidentiality	Integrity	Availability	Authenticity	Non-repudiation
Healthcare-related Data	High	High	Low	High	High
Critical Meta Data	High	High	Low	High	High
Non-critical personal data	Moderate	Moderate	Low	Moderate	Moderate
Administrative Data	Low	Low	Low	Low	Low

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.2 e1-FLD-147 Security requirements

Although a detailed risk analysis could not be performed due to time limitations, a detailed study has been made of the epSOS LSP data and processes, and more specifically of the Organizational requirements, the Legal requirements, the Technical requirements, the Security Audit requirements, the user requirements, etc. Based on those security requirements and the security best practices in the field of health, the following epSOS LSP security requirements have been identified.

The aim is to describe, at high level, the epSOS LSP security requirements. Following the logical architecture of the project and taking care of the complexity and the number of different approaches of the PNs, it would seem to be useful to divide the security requirements into three levels:

1st level - Security requirements for the epSOS LSP Project as a whole (that is "environmental" requirements). These requirements derive mainly from Annex I and WP2-deliverables.

2nd level - Security requirements for a National Contact Point (NCP), starting from the observation that each NCP must exchange information -in a standard way- with all the others NCPs. These requirements derive mainly from the WP3.6/WP3.2/WP3.1 deliverables the "Concept paper final" document and ISO/IEC 27000 baseline safeguards catalogue.

3rd level – Minimum acceptable common security requirements for the different National Information Infrastructure, starting from the observation that different levels of security requirements may have been established by the different Health Care National Systems. "Minimum" because they represent the minimum that satisfies the Project; "acceptable" because they are already implemented or they can be easily implemented by all PNs.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.2.1 e1-REQ-1725 Security requirements for the epSOS LSP Project level.

The epSOS LSP Project must guarantee the security of health-care data processing. This means that confidentiality, availability and integrity of data must be guaranteed through suitable security requirements. More precisely, the security requirements for the epSOS LSP Project as a whole must guarantee the following items:

Identification;

Authentication;

Access control;

Non repudiation;

Data confidentiality;

Data availability;

Logging of any operation, performed by whatever User(Active Actors), which has an impact on security.

Taking into account the indication given in the documents referred as [01], [02], [04] in the referring document list (see cover), enclosed here is a more detailed list of security requirements for epSOS LSP Project.

Please note that "MUST" is used when the requirement is **mandatory**, while "SHOULD" is used when the requirement is **recommended** but not mandatory.

In this document ,following the ITSEC definition, Accountability means: "requirements to ensure that relevant information is recorded about actions performed by users or processes acting on their behalf so that the consequences of those actions can later be linked to the user in question, and the user held accountable for his actions". **Auditing** means: "requirements to ensure that sufficient information is recorded about both routine and exceptional events that later investigations can determine if security violations have actually occurred, and if so what information or other resources were compromised".

2.2.1.2.2 e1-REQ-1728 EpSOS-Req#3.7.01 (Identification)

For each epSOS LSP Actor a valid and unique electronic identity MUST be established. The standards to which this is unique/valid MUST be established by agreement.

2.2.1.2.3 e1-REQ-1729 EpSOS-Req#3.7.02 (Authentication)

The identity of epSOS LSP Users (before each system access, transaction or message) MUST be validated.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.2.4 e1-REQ-1730 EpSOS-Req#3.7.03 (Robustly Authenticating Users)

Each MS MUST robustly grant the authentication of his own Users. The conditions on which a single MS may guarantee the User authentication, may be based on technical and/or organizational measures. These measures, in any case, SHOULD provide that the authenticated entity MUST not be repudiated.

2.2.1.2.5 e1-REQ-1731 EpSOS-Req#3.7.04 (Access control)

The confidentiality and integrity of epSOS LSP information assets MUST be protected by preventing unauthorised access and use. (protection from both the technical and organizational point of view).

2.2.1.2.6 e1-REQ-1732 EpSOS-Req#3.7.05 (Access control, privilege management and HCP authorization)

The authorization with which an identified and authenticated Health Care Professional can get access to epSOS medical information (Patient Summary & ePrescription) of a Patient MUST be based on the role assigned to the HCP (as defined by the Health-care MS organization or authority), on the verification of the parent health-care Organization, on the fact that "that" HCP is treating "that" Patient.

2.2.1.2.7 e1-REQ-1733 EpSOS-Req#3.7.06 (Confidentiality)

The unauthorized disclosure of personal medical information during the transfer, processing and storage within epSOS LSP MUST be strongly prevented. The use of cryptographic mechanisms SHOULD be adopted.

2.2.1.2.8 e1-REQ-1734 EpSOS-Req#3.7.07 (System and data integrity)

The integrity of data within epSOS LSP documents, transactions or messages MUST be assured for both data rest and transit.

2.2.1.2.9 e1-REQ-1735 EpSOS-Req#3.7.08 (Availability)

It MUST be ensured that information assets are, according to the service level agreements agreed, available in a timely and reliable manner when needed in the scope of their professional activity by authorised epSOS Users and systems.

2.2.1.2.10 e1-REQ-1736 EpSOS-Req#3.7.09 (Non Repudiation)

It MUST be ensured that both the User-Originator and the User-Receiver of documents and messages cannot deny their actions (documents production, message sending, message receiving).

2.2.1.2.11 e1-REQ-1737 EpSOS-Req#3.7.10 (Accounting)

It MUST be ensured that each activity of a User is accounted for. In any case accounting information MUST not include personal health care data.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.2.12 e1-REQ-1738 EpSOS-Req#3.7.11 (Auditing)

It MUST be ensured that each action which has an impact on security or privacy must be audited. In any case auditing information must not include epSOS personal health care data.

2.2.1.2.13 e1-REQ-1739 EpSOS-Req#3.7.12 (Fraud detection):

epSOS LSP SHOULD provide tools able to discover possible frauds in the use of medical data.

2.2.1.2.14 e1-REQ-1740 EpSOS-Req#3.7.13 (Traceability)

It MUST be ensured that log data can be connected from different sources in a privacy-compliant way.

2.2.1.2.15 e1-REQ-1741 EpSOS-Req#3.7.14 (End-of-Life process)

A process MUST be developed by each MS on when and how to destroy all data objects created for the epSOS LSP after its conclusion.

2.2.1.2.16 e1-REQ-1742 EpSOS_Req#3.7.15 (Privacy)

Each epSOS LSP Data Controller MUST guarantee the respect of the privacy obligations foreseen by its National Law and the European Directive 95/46/EC.

2.2.1.2.17 e1-REQ-1743 EpSOS-Req#3.7.16 (Trust)

Each MS SHOULD show evidences of the respect, by its own health-care information system, of the security requirements established by the pilot sites agreement.

2.2.1.2.18 e1-REQ-1726 Security requirements for a National Contact Point (NCP) level.

Taking into account the indications given in doc#3 in the referring document list, the list of the security requirements at epSOS LSP Project level (see previous paragraph), and the ISO/IEC 27002 baseline safeguard catalogue, enclosed here is a more detailed list of security requirements for a National Contact Point.

Please notice that "MUST" is used when the requirement is mandatory, while "**SHOULD**" is used when the requirement is recommended but not mandatory.

2.2.1.2.18.1 e1-REQ-1744 NCP-Req#3.7.01a (NCP identification)

A NCP MUST have a unique electronic identity in a common cryptographic domain (such as, for example, digital certificates following x509 Standard).

2.2.1.2.18.2 e1-REQ-1745 NCP-Req#3.7.01b (NCP local User I&A)

I&A of each local User (NCP technical staff) MUST be performed before he/she starts processing. The tool/mechanism used (individually or with other security tools/mechanisms/procedures) for I&A MUST prevent the User's identity (previously submitted to I&A) from being repudiated.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.2.1.2.18.3 e1-REQ-1746 NCP-Req#3.7.02 (Authenticating Network Access)

Each NCP MUST ensure that all connections to remote servers (both other NCPs and local systems) and applications are authenticated.

2.2.1.2.18.4 e1-REQ-1747 NCP-Req#3.7.03a (Digital Signatures)

If in a MS the epSOS LSP Users apply a digital signature, then the MS-related NCP MUST be able to:

verify that the digital signature is valid (this implies that the user certificate is also valid)

confirm that validity to any other MS-NCP, through a digital signature.

2.2.1.2.18.5 e1-REQ-1748 NCP-Req#3.7.03b (Digital Signatures)

If a MS does not adopt a digital signature, then the MS-related NCP MUST be able in any case to:

confirm to any other MS-NCPs connecting, the data integrity of the exchanged data through a digital signature.

2.2.1.2.18.6 e1-REQ-1749 NCP-Req#3.7.04 (Access Control)

A NCP MUST provide Access Control mechanisms which provide functionalities that allow, for a given User, the specification of which data and services the User can get access to, and which privileges the User has with regard to the data and services.

2.2.1.2.18.7 e1-REQ-1750 NCP-Req#3.7.05 (Confidentiality)

A NCP MUST use strong cryptographic mechanisms to prevent the unauthorized disclosure of personal medical information or security critical system data during the transfer and processing within the NCP itself if this processing has confidentiality vulnerabilities.

2.2.1.2.18.8 e1-REQ-1751 NCP-Req#3.7.06 (Protecting Source and Destination Integrity during data transmission)

The source and destination of the message during data transmission between NCPs MUST be protected to maintain its integrity.

2.2.1.2.18.9 e1-REQ-1752 NCP-Req#3.7.07 (Protecting Data Storage)

If storage is performed, a NCP MUST protect medical information or security critical system data it contains. The use of pseudo-anonymization mechanisms SHOULD be used if possible or reasonable.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.2.18.10 e1-REQ-1753 NCP-Req#3.7.08 (System and data integrity)

A NCP MUST ensure, by strong cryptographic mechanisms, the ability to discover if the medical information has been altered or destroyed in a unauthorized manner, so that that medical information may not be further processed.

2.2.1.2.18.11 e1-REQ-1754 NCP-Req#3.7.09 (Availability)

NCP best effort MUST ensure the respect of the agreed Service Level Agreements.

2.2.1.2.18.12 e1-REQ-1755 NCP-Req#3.7.10(Non Repudiation)

A NCP MUST have a strong cryptographic mechanism (i.e. RSA) to ensure the non repudiation of each document produced by itself or messages exchanged with other NCPs.

2.2.1.2.18.13 e1-REQ-1756 NCP-Req#3.7.11 (Accounting and Control)

A NCP MUST have a mechanism to record every access request and disclosure of medical information and clinical data, together with the time and identity of the accessing User. Clinical data MUST NOT be included in accounted data. Accounting records MUST be maintained as long as the pilot project lasts, unless otherwise legally required.

2.2.1.2.18.14 e1-REQ-1757 NCP-Req#3.7.12 (Auditing)

It **MUST** be ensured that each action which has an impact on security is recorded. If data to be recorded contain both medical and personal data, an anonymization or pseudo-anonymization process **SHOULD** be used if possible or reasonable. In any case the recorded data **MUST** not contain personal health care data, but can contain a unique identifier to a data object. Audit records **MUST** be maintained as long as the pilot project lasts, unless otherwise legally required.

2.2.1.2.18.15 e1-REQ-1758 NCP-Req#3.7.13 (fraud detection)

NCP MUST provide tools to discover possible frauds in the use of medical data.

2.2.1.2.18.16 e1-REQ-1759 NCP-Req#3.7.14 (Continuously Logging)

Logging on the NCP **SHOULD** be operational at all times. In case of failure, the NCP involved **MUST** inform all the other NCPs.

2.2.1.2.18.17 e1-REQ-1760 NCP-Req#3.7.15 (Securing Access to Audit/Account Logs)

A NCP **MUST** secure the access to audit records to prevent misuse or compromise.

2.2.1.2.18.18 e1-REQ-1761 NCP-Req#3.7.16 (Logging Transactions)

A secure audit record **MUST** be created each time a User asks to access medical information of a Patient or to send an e-prescription dispensation's notification.

2.2.1.2.18.19 e1-REQ-1762 NCP-Req#3.7.17 (Trust)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

It SHOULD be allowed to submit each NCP to a "second part" (see ISO 9000) security audit procedure performed by the other MS, so that it will be possible to verify the compliance with the security requirements established by the pilot sites agreement.

2.2.1.2.18.20 e1-REQ-1763 NCP-Req#3.7.18 (Minimum Content of Accounting Logs)

The logs SHOULD contain:

the user ID of the accessing User;

the role the User is exercising;

the organisation of the accessing User (at least in those cases where an individual accesses information on behalf of more than one organisation);

the unique Patient ID;

the function performed by the accessing User;

the NCP-id of the Originator/Target;

a time stamp including time zone used.

2.2.1.2.18.21 e1-REQ-1764 NCP-Req#3.7.19 (Reporting Every Access medical information, notifications included)

It SHOULD be possible to identify all requests to access to any Patient's record(s) (dispensations and modifications included) over a given period of time according to different parameters (Users, Patients' records,...)

2.2.1.2.19 e1-REQ-1765 Environmental and operational NCP security requirements.

It is strongly recommended that the following security requirements SHOULD be met by all NCPs engaged in the epSOS pilot phase.

2.2.1.2.19.1 e1-REQ-1775 NCP-Req#3.7.20 (Personnel security – security in job definition and resourcing)

Security responsibilities for technical staff, data security officer and auditor SHOULD be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment. All employees and third party users of information processing facilities SHOULD sign a confidentiality (non-disclosure) agreement.

2.2.1.2.19.2 e1-REQ-1776 NCP-Req#3.7.21 (Personnel security – user training)

Technical staff SHOULD be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.2.19.3 e1-REQ-1777 NCP-Req#3.7.22 (Personnel security – Responding to security incidents and malfunctions)

Incidents affecting security MUST be reported to the designated (by each MS) point of contact through appropriate management channels as quickly as possible.

2.2.1.2.19.4 e1-REQ-1778 NCP-Req#3.7.23 (Personnel security – Responding to security incidents and malfunctions)

All employees and contractors MUST be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of NCP assets. They MUST be required to report any observed or suspected incidents as quickly as possible to the designated (by each MS) point of contact.

2.2.1.2.19.5 e1-REQ-1779 NCP-Req#3.7.23 (Physical and Environmental security – secure areas)

Critical or sensitive information processing facilities SHOULD be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They MUST be physically protected from unauthorized access, damage and interference.

2.2.1.2.19.6 e1-REQ-1780 NCP-Req#3.7.24 (Physical and Environmental security – secure areas)

The protection provided SHOULD be commensurate with the identified risks.

2.2.1.2.19.7 e1-REQ-1781 NCP-Req#3.7.25 (Physical and Environmental security – equipment security)

Equipment SHOULD be physically protected from security threats and environmental hazards. Protection of equipment is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also take into consideration equipment location and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

2.2.1.2.19.8 e1-REQ-1782 NCP-Req#3.7.26 (Physical and Environmental security – general controls)

Information and information processing facilities SHOULD be protected from disclosure, modification or theft by unauthorized persons, and controls SHOULD be in place to minimize loss or damage.

2.2.1.2.19.9 e1-REQ-1783 NCP-Req#3.7.27 (Communications and operations management - Operational procedures and responsibilities)

Responsibilities and procedures for the management and operation of information processing facilities MUST be established. This includes the development of appropriate operating instructions and incident response procedures.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.2.19.10 e1-REQ-1784 NCP-Req#3.7.28 (Communications and operations management - System planning and acceptance)

The operational requirements of new systems SHOULD be established, documented and tested prior to their acceptance and use.

2.2.1.2.19.11 e1-REQ-1785 NCP-Req#3.7.29 (Communications and operations management - Protection against malicious software)

Precautions SHOULD be required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs.

2.2.1.2.19.12 e1-REQ-1786 NCP-Req#3.7.30 (Communications and operations management - Housekeeping)

Routine procedures SHOULD be established for carrying out the agreed back-up strategy taking back-up copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment.

2.2.1.2.19.13 e1-REQ-1787 NCP-Req#3.7.31 (Communications and operations management – Network management)

The security management of networks which span organizational boundaries requires attention. Additional controls may also be required to protect critical data passing over public networks.

2.2.1.2.19.14 e1-REQ-1788 NCP-Req#3.7.32 (Communications and operations management – Media handling and security)

Media SHOULD be controlled and physically protected. Appropriate operating procedures SHOULD be established to protect documents, computer media (tapes, disks, and cassettes), input/output data and system documentation from damage, theft and unauthorized access.

2.2.1.2.20 e1-REQ-1727 Acceptable common security requirements for the different National Information Systems (NIS) level

The acceptable security requirements for the different National Information Infrastructure derive from the requirements listed in the previous paragraphs, the analysis of the answers to the questionnaire (see following chapter) and –in any case- must be compliant with the EU directive for data protection.

Please notice that "MUST" is used when the requirement is **mandatory**, while "SHOULD" is used when the requirement is **recommended** but not mandatory.

2.2.1.2.20.1 e1-REQ-1766 NIS-Req#3.7.01 (Identity and Authorization of a User)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

I&A of a User MUST be performed before he/she starts processing. The tool/mechanism used (individually or with other security tools/mechanisms/procedures) for I&A MUST prevent the User's identity (previously submitted to I&A) from being repudiated.

2.2.1.2.20.2 e1-REQ-1767 NIS-Req#3.7.02 (Access Control)

An Access Control tool/mechanism which enables access to medical information on the basis of the User Identity and the role (and related authorizations) he/she plays, MUST exist.

2.2.1.2.20.3 e1-REQ-1768 NIS-Req#3.7.03 (Confidentiality and Integrity)

Confidentiality and integrity of the medical informations produced, sent or stored, MUST be guaranteed. Data SHOULD be protected by the use of acknowledged (by the single MS) cryptographic algorithms.

2.2.1.2.20.4 e1-REQ-1769 NIS-Req#3.7.04 (Audit & Accounting)

A process which allows the collection and the consultation of the information of both the actions performed by the Users and the events which impact on security, MUST exist. All the data collected MUST be protected from unauthorized access.

2.2.1.2.20.5 e1-REQ-1770 NIS-Req#3.7.05 (Limiting Use and Disclosure of Personal Health Information to Identified Purposes)

Organisations connecting to the epSOS LSP and organisations hosting components of the epSOS LSP MUST only use or disclose medical information for purposes consistent with those for which it was collected, except in the case of Patient consent or if permitted (or required) by law.

2.2.1.2.20.6 e1-REQ-1771 NIS-Req#3.7.06 (Segregating Network Users, Services and Systems)

Organisations hosting epSOS LSP components MUST introduce network controls to segregate information services, Users and information systems that are not involved in access to or hosting of the epSOS LSP systems. Separated management networks are recommended.

2.2.1.2.20.7 e1-REQ-1772 NIS-Req#3.7.07 (Privacy)

Each epSOS LSP Data Controller MUST guarantee the respect of the privacy obligations foreseen by its National Law.

2.2.1.2.20.8 e1-REQ-1773 NIS-Req#3.7.08 (Trust)

Each MS SHOULD show evidence of the respect, by its own health-care information system, of the security requirements established by the pilot sites agreement.

2.2.1.2.20.9 e1-REQ-1774 NIS-Req#3.7.09 (Protecting Against Malware)

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

Each MS IT-system involved in the epSOS LSP Project MUST implement, according to ISO/IEC 27000, appropriate detection and prevention controls to protect against malicious software (viruses, worms, etc):

Reference to page 126/127 of epSOS annex 1

"detailed approach", "informal approach", "combined approach" and "baseline approach" are definitions of ISO/IEC TR 13335-3 (see doc#8 in the referring list document).

2.2.1.2.21 e1-REQ-4591 REQ 3.3.6 Secure Context Establishment

Related to e1-REQ-4564 NFR09- Trust between countries

Related to e1-REQ-4565 NFR09- Trust between countries

Related to e1-REQ-1835 epSOS Audit Trail Common Specification

Related to e1-REQ-1899 epSOS Profiles on Assertions and Certificates

Related to e1-REQ-4614 Process secure context establishment between 2 NCPs

Related to e1-REQ-1879 Trusted Node Infrastructure

Business transactions rely on a secure context (session). All communications must be encrypted.

Secure Context Establishment supports the separation of basic security concerns from the business transactions. This shall be achieved by defining a secure context that the business transactions can rely on. Before an epSOS transaction is carried out on business level, a secure context between the involved actors shall be established.

Considering the potential number of exchanges for the LSP (epSOS), a stateless processing MUST be used at business level. Explicit sessions with session identifiers exchanged for the application layer are out of scope.

The communication between 2 NCPs:

MUST include mutual NCP-B/NCP-A authentication (unique and non-repudiable identification) and MUST prevent attacks on the communication level,

MUST include mechanisms for confidentiality, integrity and non-repudiation,

MUST provide a unique identification and a non-repudiable authentication of HP,

MUST provide means to make a business request non-repudiable for the HP,

MUST ensure that the originator information of a medical data object is authentic,

MUST ensure that a medical data object has not been modified while transmitted.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.2.22 e1-REQ-4605 REQ 3.3.20 NCP Signatures

NCP signatures shall be used to vouch for the authenticity of exchanged data. If a medical data is signed by the HP, this signature MUST be verified.

NCP-B signature shall be used for each request sent from NCP-B to NCP-A, and the validity of this signature shall be checked on the NCP-A side.

2.2.1.2.23 e1-REQ-4609 REQ 3.3.24 Transaction consistency confirmation

The system must provide confirmation that a complete data set has been transmitted. An alert should signal any interruption or fault which may have resulted in some data being omitted.

2.2.1.2.24 e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-1960 Compliance to European Legislation

Related to e1-REQ-1970 Consent Registration

Related to e1-REQ-4429 REQ 3.6.26 Withdrawing patient consent

Synchronized with e1-REQ-3866 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-4541 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-5089 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-5090 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-5091 Willful Provisioning of Data (»Consent-1«)

The provisioning of medical data for cross-border medical use cases MUST require a willful and documentable act of agreeing by the patient.

This willful act MUST fulfill all requirements of an informed, free consent acc. to country-A legislation. It MUST deliver an appropriate level of data security and privacy for the patient as it is defined in his home country.

This willful act MUST be designed in full anticipation of a cross-border health data exchange scenario.

The respective consent MUST be given in written form and MUST be signed by the patient. A qualified digital signature MAY be used instead of a wet signature.

A country MUST assure that patient data is only accessible if a valid patient consent for data provisioning exists. A country MUST ensure that data is no longer accessible after the respective consent has been revoked or expired.

A HP- B is not required to explicitly verify the existence of a patient's »consent-1« (that was formerly given in country-A) as it is assumed that all epSOS country-A have established secure processes for enforcing the revocation of consents and therefore will not provide data to a country-B unless a valid »consent-1« exists.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.2.1.2.25 e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-1960 Compliance to European Legislation

Related to e1-REQ-1977 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-3867 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-4542 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-5092 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-5093 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-5094 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-4876 Documentation of the Patient Information Notification (PIN)

Triggering a cross-country transfer of medical data MUST require a willful act by the patient.

This willful act MUST express the patient's explicit authorization to allow an identifiable healthcare professional the execution of defined data access operations.

This willful act MUST express the explicit authorization of the patient to transfer medical data to the formerly identified and specifically documented destination.

Countries MAY require that this willful act is documented by an explicit, written and informed consent that is to be signed by the patient.

Implications:

The authorization to perform a specific operation can only be given and documented in country-B (as this authorization requires the identification of both the patient and the HP-B).

Therefore epSOS MUST provide technical means to transmit information about the authorization/PIN to country-A before or while a data access operation is triggered.

2.2.1.2.26 e1-REQ-1976 Needs-to-Know-Principle

Related to e1-REQ-1960 Compliance to European Legislation

Related to e1-REQ-2217 L-DP-07 Proportionality and purpose limitation

Country-B MUST ensure that requests which are forwarded to a country A reflect a business need which matches the role (and/or other properties) of the requestor.

Country-B MUST NOT forward requests to country-A unless they are compliant to country-B legislation. Country-B SHOULD provide country-A with information on the permissions of HP-B within country-B in order to enable country-A to override its national security policy with country-B permissions.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Implication:

Country-B MUST enforce its national security policy before a request is sent to country-A. HP permissions SHOULD be provided to country-A as part of every request that is sent to country-A.

2.2.1.2.27 e1-REQ-1977 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-1960 Compliance to European Legislation

Related to e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-3889 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-4560 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-5085 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-5086 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-5088 Willful Disclosure (Data Confidentiality)

Medical data MUST NOT be disclosed to persons or organization unless they have been authorized by the patient (see »Consent-2; PIN«) and the disclosure is legally or explicitly required for fulfilling the treatment.

Medical data MUST NOT be disclosed to others than healthcare professionals or healthcare professional organizations in any case.

Medical data MUST NOT be transferred to other destinations unless this disclosure has been authorized by the patient or is mandated by national law.

The proper enforcement of the willful disclosure acc. to »consent-2« MUST be controllable and verifiable by the patient.

Implications:

Data MUST be encrypted during transfer and whenever it is stored at (intermediate) nodes outside the trusted environment of an HP (see "IT-Systems directly controlled by HPs").

Depending on how "controllable" and "verifiable" are defined this requirement as well implies a need for secure end-to-end encryption between trusted HP environments.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.2.28 e1-REQ-1978 Data Integrity

Related to e1-REQ-1960 Compliance to European Legislation

Related to e1-REQ-1961 Patient Safety

Synchronized with e1-REQ-3888 Data Integrity

Synchronized with e1-REQ-4558 Data Integrity

Synchronized with e1-REQ-5105 Data Integrity

Synchronized with e1-REQ-5106 Data Integrity

Synchronized with e1-REQ-5107 Data Integrity

Synchronized with e1-REQ-5108 Data Integrity

Related to e1-REQ-1879 Trusted Node Infrastructure

The integrity of transmitted data MUST be preserved when information is transmitted between different entities (legally or technically defined). It must be verifiable to a data receiver that data has not been damaged, altered or (partially) lost.

2.2.1.2.29 e1-REQ-1979 Data Minimization

Related to e1-REQ-1960 Compliance to European Legislation

Cross-border exchange of medical data MUST minimize the amount of personal data that is disclosed and processed in both country A and B.

Cross-border exchange of medical data MUST NOT require the collection or processing of personal data beyond the minimum amount of the envisioned medical purpose, its digital evidence, its administration, accompanying patient safety aspects, and regulatory provisions, such as mandatory disclosure requirements of key indications, performance and quality assurance) in the affected countries.

Pseudonyms SHOULD be used whenever possible unless this may impose risks to patient safety (e.g. false assignment of data, unacceptable restriction of returning vital medical information).

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.2.1.2.30 e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-1960 Compliance to European Legislation

Related to e1-REQ-2212 L-LI-01 Traceability

Related to e1-REQ-4960 Audit and Accounting

Synchronized with e1-REQ-3872 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-4671 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-5080 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-5081 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-5082 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-5083 Traceability and Exercise of Patient Information Rights

Cross-border exchange of medical data MUST be documented in a fully traceable, reconstructable, and seamless fashion.

Cross-border exchange of medical data MUST produce a usable chain of digital evidence that enables both, the patient and his assigned DPA, to pursue, enforce, and proof any assumed or detected violation of the patient's data protection and privacy rights.

The chain of digital evidence MUST disclose the minimum of personal health data required to serve its purpose and MUST be specifically safeguarded against wrongdoing. Part of these safeguards MUST be a protocol that is not accessible to HPs.

Implications:

Audit trails SHOULD be written at both NCPs. For the purpose of data minimization NCP audit trails SHOULD not include medical data but just refer to (and safeguard) respective audit trails within HP systems.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.2.1.2.31 e1-REQ-1981 HP-B Identification and Authentication

Related to e1-REQ-1901 HCP Identity Assertion

Synchronized with e1-REQ-3863 HP-B Identification and Authentication

Synchronized with e1-REQ-4538 HP-B Identification and Authentication

Synchronized with e1-REQ-4991 HP-B Identification and Authentication

Synchronized with e1-REQ-5076 HP-B Identification and Authentication

Related to e1-REQ-4602 REQ 3.3.17 HP-B authentication at NCP-B

Related to e1-REQ-1902 Treatment Relationship Confirmation Assertion

The identity and authenticity of an HP MUST be verified before he can use epSOS cross-border services. Each data access request MUST contain sufficient and verifiable information about (the identity and the role of) the accessory for assessing a country-A national security policy.

2.2.1.2.32 e1-REQ-1984 Data Origin and Data Authenticity

Related to e1-REQ-1961 Patient Safety

Related to e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Synchronized with e1-REQ-4411 Data Origin and Data Authenticity

Synchronized with e1-REQ-4563 Data Origin and Data Authenticity

Synchronized with e1-REQ-5119 Data Origin and Data Authenticity

Synchronized with e1-REQ-5120 Data Origin and Data Authenticity

Synchronized with e1-REQ-5121 Data Origin and Data Authenticity

The intended recipient of a medical data communication MUST be able to determine the originator and level of authenticity of the medical data received. Information on the identity and authenticity of the data originator that is assigned to the data or its metadata MUST NOT be altered during cross-border transfer.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.2.1.2.33 e1-REQ-1985 Patient Data Assignment

Related to e1-REQ-1961 Patient Safety

Related to e1-REQ-1968 Provisioning of Medical Data by Country A

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Related to e1-REQ-4846 Unique Patient Identifier

The user of medical data MUST be able to unambiguously assign medical data (that is obtained from another country) to an identified patient.

Information on the identity of the patient that is assigned to the data and/or its metadata MUST NOT be altered in-band during a cross-border transfer.

Any identity abstraction or alteration, such as the assignment of pseudonyms, MUST be performed by country A in order to guarantee the correct linkage of medical data to a specific identity regardless of its characteristics (pseudonym, MIP or domain identifier).

2.2.1.2.34 e1-REQ-4454 REQ 3.6.14 Audit log encryption

Audit Log must be encrypted.

2.2.1.2.35 e1-REQ-4960 Audit and Accounting

Related to e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-4636 NCP Audit Trial Interface and Functionality

The following requirement shall be taken into consideration when implementing this security service:

the audit systems (Log data server) must be segregated from the audited system (epSOS-NCP) itself;

the epSOS-NCP has to be provided with an agent which sends audit data in real time to a secured Log data server;

Log data format will follow indications in RFC3881 (Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications).

the secured Log data server may store received data and relative hash or digital signature on a worm (Write Once Read Many) device, or equivalent method, to prevent offline tampering and deleting;

the system administrators and the HPs must be distinct people with no hierarchical relationship between them

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

On the Log data server, a statistical analysis via business intelligence or data mining products, of the Logged data has to be provided in order to allow early discovery of any misused or fraudulent use of epSOS. (using commercially available products, to be customized, such as Oracle Data Mining or Business Objects)

Every data Logged Must in every case be compliant with the following requirements:

For every transaction, stored information may include information contained both in the request and in the response.

For every record created by the Audit system, a timestamp of date and time must be recorded from time services, which ensures synchronization between different countries.

HP and Patient IDs are not immediately associative with the personal information of their owners because this kind of information is not stored on the secure audit system. Should any information stored in the audit system lead to patient identification, such information MUST be kept in separated tables from the ones containing the IDs identifying transactions and operations.

The purpose of the audit system is not to store healthcare-related data within the transactions, which is why this type of data should not be stored in any way on the systems.

However, since the system may be able to provide evidence that a transaction has been requested or not, a cryptographic function (ie hash or the encryption in a way that the decrypting key should not be under the direct control of the NCP) of the health/health-related transmitted data may be stored.

The data Log MUST NOT be used for different purposes than:

to analyze or to prevent a breach of security;

to respond to the right request of the data subject (patient) or to “National entities” legally authorized, with the aim of providing the evidence necessary to the case.

Finally, to ensure that logs would not be tampered with, a sign mechanism to sign every log record may be adopted. On top of this a sign mechanism of the whole daily list of log entries can be put in place in order to ensure integrity of the entire dataset.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.2.1.2.35.1 e1-REQ-4961 Audit Scope and Events

All these events MUST be logged independently for the result (successful or not) of the corresponding action.

HP Authentication

Patient Identification and Authentication

HP Authorization

Medical data Query and Retrieve

Medical Data Update (Dispensation notification)

Moreover the NCP secure audit system has to LOG the following system and network infrastructure events:

NCP / Security Service start up/shut down;

Usage of secure Audit log (other than audit log record creation);

Access policy change (ie. Network, file system);

User account event (ie. Create account);

Configuration changes;

Partial failure;

PKI event;

Timing synchronization;

Authentication (NCP, Technical Staff) failure and success

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.2.35.2 e1-TXT-774 Note

Audit is defined as the analysis of actions and states of a system or a user. This implies gathering complete and time-referenced information about the actions related to the system that has to be audited.

The means used to keep track of this information is called "Log". Logs are therefore evidence of any kind that can provide support to the audit.

Because during the analysis of the Logs, when applicable, it's important to clearly identify "who" has performed the action (accountability), to make it possible, the user' (active epSOS entity) must be identified and authenticated.

EpSOS provides processing and transmission of health data that has legal implications for the actors involved in the system, for these reasons it's also important to audit transactions to identify any deficiencies related to security.

The objective of Audit and Accounting security service is to provide a history of transactions and to ensure that it is possible to trace who has performed any action involving a epSOS-NCP transaction.

2.2.1.2.35.3 e1-REQ-4962 Prevention of data deletion

The service MUST ensure to be tamper-proof to avoid the historical data to be deleted or tampered with, even by Technical Staff (system administrators).

2.2.1.2.35.4 e1-REQ-4963 Secure storage of audit trails

The system devoted to audit collection must guarantee a high degree of security itself, both from the data transmission and data storing point of view.

The following requirements must be satisfied:

the PHYSICAL system(s) hosting the audit collection processes and the audit data (logs) must be physically protected (closed environment, access control);

the MACHINE(s) hosting the audit collection processes and the audit data (logs) must be UNACCESSIBLE by Technical staff users;

users allowed/entitled to access the audit system will ONLY have the right to access in READING the logs, without having access to other system functions

audit data (logs) must be stored on non-modifiable supports (WORM) or equivalent method;

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

communication between epSOS-NCP and the Audit trails secure storage should be secured and both systems should also authenticate each others.

2.2.1.2.35.4.1 e1-REQ-4964 Relaxation for pilot phase

To reduce the cost and the complexity of the epSOS NCP technical implementation, the requirement for a separate secure storage of audit trails may be relaxed.

The waiver of a separate secure storage system must be compensate by specific organizational and procedural security measures, and must be confirmed by a risk analysis.

2.2.1.2.35.5 e1-REQ-4965 EpSOS-Req#3.7.10 (Accounting)

It MUST be ensured that each activity of a User is accounted for. In any case accounting information MUST not include personal health care data.

2.2.1.2.35.6 e1-REQ-4966 EpSOS-Req#3.7.11 (Auditing)

It MUST be ensured that each action which has an impact on security or privacy must be audited. In any case auditing information must not include epSOS personal health care data.

2.2.1.2.35.7 e1-REQ-4967 EpSOS-Req#3.7.12 (Fraud detection)

epSOS LSP SHOULD provide tools able to discover possible frauds in the use of medical data.

2.2.1.2.35.8 e1-REQ-4968 NCP-Req#3.7.11 (Accounting and Control)

A NCP MUST have a mechanism to record every access request and disclosure of medical information and clinical data, together with the time and identity of the accessing User. Clinical data MUST NOT be included in accounted data. Accounting records MUST be maintained as long as the pilot project lasts, unless otherwise legally required.

2.2.1.2.35.9 e1-REQ-4969 NCP-Req#3.7.12 (Auditing)

It MUST be ensured that each action which has an impact on security is recorded. If data to be recorded contain both medical and personal data, an anonymization or pseudo-anonymization process SHOULD be used if possible or reasonable.

In any case the recorded data MUST not contain personal health care data, but can contain a unique identifier to a data object.

Audit records MUST be maintained as long as the pilot project lasts, unless otherwise legally required.

2.2.1.2.35.10 e1-REQ-4970 NCP-Req#3.7.13 (fraud detection)

NCP MUST provide tools to discover possible frauds in the use of medical data.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.2.35.11 e1-REQ-4971 NCP-Req#3.7.14 (Continuously Logging)

Logging on the NCP SHOULD be operational at all times. In case of failure, the NCP involved MUST inform all the other NCPs.

2.2.1.2.35.12 e1-REQ-4972 NCP-Req#3.7.15 (Securing Access to Audit/Account Logs)

A NCP MUST secure the access to audit records to prevent misuse or compromise.

2.2.1.2.35.13 e1-REQ-4973 NCP-Req#3.7.16 (Logging Transactions)

A secure audit record MUST be created each time a User asks to access medical information of a Patient or to send an e-prescription dispensation's notification.

2.2.1.2.35.14 e1-REQ-4975 NCP-Req#3.7.19 (Reporting Every Access medical information, notifications included)

It SHOULD be possible to identify all requests to access to any Patient's record(s) over a given period of time according to different parameters.

2.2.1.2.35.15 e1-TXT-775 Audit and Accounting Option Analysis

ATNA accepts two possible solutions as Audit record transportation between epSOS NCP and the data Log server:

Transmission of syslog message (Log record) over TLS (RFC5425) with the syslog protocol (RFC5424).

Transmission of syslog message (Log record) over UDP (RFC5426) with the syslog protocol (RFC5424).

The advantage of the former solution is related to the security (confidentiality and integrity) of the TLS protocol, but as contra, in case of protocol failure, delay or block of the epSOS NCP primary functions may occur. To avoid this situation a specific recovery procedure must be adopted with complexity and increasing cost.

The latter solution has the advantage of being easier to implement, and having a better performance, UDP being a stateless protocol, any fault of the protocol has no impact on epSOS NCP.

As a drawback this solution does not guarantee the confidentiality and the integrity of the message (a log record may be missed without notice). The drawback may be reduced by implementing a read after write strategy, and adopting a dedicated point to point connection between epSOS-NCP and the data Log server.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

The adoption of UDP protocol with the suggested safeguards seems to be a better solution for the piloting phases of the epSOS LSP.

2.2.1.2.36 e1-REQ-4977 EpSOS-Req#3.7.04 (Access control)

Related to e1-REQ-4981 Process Access Control with epSOS Use Cases

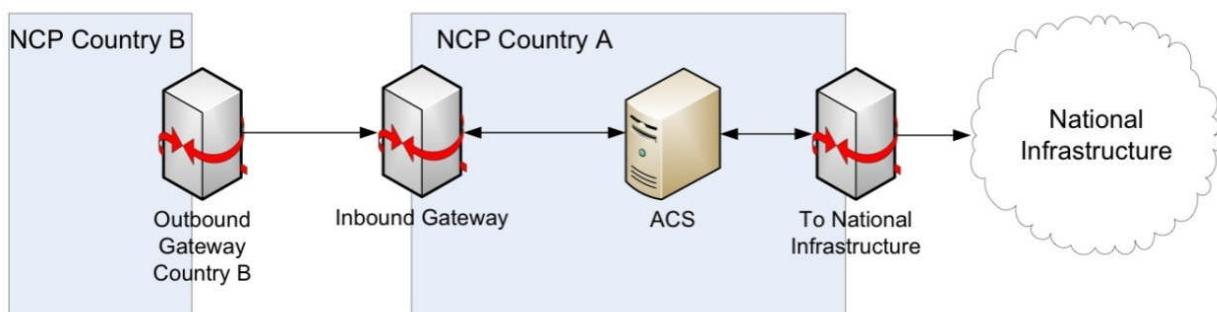
The confidentiality and integrity of epSOS LSP information assets MUST be protected by preventing unauthorised access and use.

2.2.1.2.36.1 e1-TXT-776 Note

The objective of the access control security service is to provide a means for the PNs to enforce access controls on resources without interfering within the local legislation, at the NCP level. Each actor involved in the access control security service (PEP, PDP, PR, and PAP) will be grouped with the NCP.

The Access Control Security Service fulfils requisite EpSOS-Req#3.7.4 because it is enforcing an access control decision prior giving access to a resource. The epSOS-Req#3.7.5 is satisfied because the access control decision is based upon the role played by the HP (as per PBAC/RBAC mechanism). The NCP-Req#3.7.4 is satisfied because the actors involved in the ACS are grouped within the epSOS-NCP, so the epSOS-NCP is providing an Access Control mechanism.

The ACS filters each request coming from the other epSOS epSOS-NCPs as illustrated in the architecture below:



	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.2.36.2 e1-REQ-4978 EpSOS-Req#3.7.05 (Access control, privilege management and HP authorization)

Related to e1-REQ-4981 Process Access Control with epSOS Use Cases

The authorization with which an identified and authenticated Health Professional can get access to epSOS medical information (Patient Summary & ePrescription) of a Patient MUST be based on the role assigned to the HP (as defined by the Healthcare PN organization or authority), on the verification of the parent healthcare Organization, on the fact that "that" HP is treating "that" Patient.

2.2.1.2.36.3 e1-REQ-4979 NCP-Req#3.7.04 (Access Control)

Related to e1-REQ-4981 Process Access Control with epSOS Use Cases

A NCP MUST provide Access Control mechanisms which provide functionalities that allow, for a given User, the specification of which data and services the User can get access to, and which privileges the User has with regard to the data and services.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.3 e1-FLD-148 Security Layer

2.2.1.3.1 e1-REQ-1793 Data Exchange Security Service

2.2.1.3.2 e1-REQ-1794 Trust Zones of epSOS

Certain components of the overall IT infrastructure (e.g. applications, systems and networks) are protected by security measures (e.g. firewalls, gateways) and form a reliable environment that can be referred to as "Trust Zone".

Depending on the measures in place, information with different protection requirements can be processed inside these environments. Therefore a trust zone describes a specific IT environment that corresponds to specific protection requirements categories (normal, high, very high). A trust zone can be a collection of applications, IT systems, the underlying network and the used infrastructure or just a single application or IT system embedded in a surrounding infrastructure. The following illustration shows a simplified network plan of the epSOS infrastructure that contains three general trust zones (which will have to be further refined):

Trust Zone characterization

Each trust zone can be characterized independently. The following table provides a coarse-grained characterization of the epSOS trust zones:

Trust Zone I. The first zone is formed by the whole internal network of a country. Basic security measures (packet filters and a dedicated internal network infrastructure) protect it from outside threats.

Trust Zone II. The second trust zone is formed by a subset of the first zone. Internal security measures like a logical and physically separated network that is only accessible through a gateway, protect the environment even from internal threats. For epSOS applications epSOS-NCP gateways act as the only entry and exit point from this zone.

Trust Zone III. Trust zone III is a subset of trust zone II. In addition to the measures that are in place to secure the second zone, additional protection is provided. This trust zone corresponds to the existing national eHealth infrastructures which are considered to be secure by definition.

Trust Zone IV. All common epSOS directories and services (e. g. for reporting and management) are located in a separated trust zone. (This zone was not included in epSOS LSP)

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Mapping protection requirements for TrustZones

The security measures that are implemented for each of the trust zones correspond to different protection requirement categories. The following table gives an overview on which protection category can be adequately addressed by which trust zone in the case of epSOS:

	Confidentiality	Integrity	Authenticity	Non Repudiation
Trust Zone I	Normal	Normal	Normal	n.a.
Trust Zone II	High	High	High	Normal
Trust Zone III	Very high	Very high	Very high	Very high

2.2.1.3.3 e1-REQ-1795 End-2-End-Security

The epSOS architecture is characterized by the presence of reusable, loosely coupled services that fulfil the specific business requirements of ePrescription and Patient Summary. The coupling of these services is realized by sending and receiving standardized messages over existing network infrastructures. Message exchange within these infrastructures can be exposed to threats concerning information confidentiality, integrity, liability (non-repudiation) and availability. Particularly with regard to the transfer of messages over public networks like the internet, mechanisms have to be identified that guarantee the complete and continuous protection of the transferred information from the sender of a message to its recipient. Continuous in this context means that no intermediary is able to compromise information security (e.g. read the content, change the content without being noticed) while the message is in transit. This concept is often referred to as "End-to-End Security".

By settling the ends of "End-to-End Security" on different abstraction layers, the requirements on safeguards and the reachable levels of security change dramatically. For the purposes of epSOS, four levels of "End-to-End Security" will be considered:

Object lifecycle: protected objects are secured throughout their lifecycle from their creation to their consumption without any gaps. E. g. in order to gain lifecycle end-to-end confidentiality for a ePrescription it must be encrypted just after signing and can only be decrypted by an authorised end user. In epSOS the ends of object lifecycle end-to-end security are the HCP in country A, who created a medical document and the HCP in country B, who used this

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

document. Object lifecycle end-to-end security is best suited for matching very high protection demands.

Business transaction: protected objects are secured all the way between two communicating business level applications. E. g. in order to gain business transaction end-to-end confidentiality for a request to an ePrescription managing system, the ePrescription must be encrypted by the managing system using a key known to the end user. In epSOS the ends of business transaction end-to-end security are the HCP in country B and the data managing service in country A. Depending on the additional environmental security measures on data processing and persistence, business transaction end-to-end security can require high and even very high protection demands.

Message exchange: protected objects are secured when they are persistently stored and when they are exchanged among communicating services. Communication can terminate on any ISO layer as long it is ensured that the way up to layer 7 is properly safeguarded. In epSOS the ends of message exchange end-to-end security are the epSOS-NCPs of country A and B. Depending on the additional environmental security measures on data processing and persistence, service call end-to-end security can require normal and even high protection demands.

Node-to-node: protection of data transmission between two network nodes, on-node processing, and persistence is considered to be independent from each other. This abstraction is only suited to fulfil normal protection demands.

Given the mapping of protection levels onto trust zones, this leads to the following propositions (see analysis of protection demands):

Medical Data Integrity: object lifecycle end-to-end security MUST be used if very high protection demands are to be fulfilled (decision making). Both ends MUST terminate in Trust Zone III (Medical Data used for decision making) or in Trust Zone II (Medical Data used for decision support).

Identifiable Data Confidentiality: at minimum message exchange end-to-end security MUST be provided. Communication MUST terminate in Trust Zone II or III.

Communication Liability: node/country level end-to-end security is sufficient. Communication MAY terminate in Trust Zone I.

Data Availability: point-to-point security is sufficient. Communication MAY terminate in Trust Zone I

Entity Authentication: at minimum message exchange level end-to-end security MUST be provided (users do not alter medical data, therefore identity theft does not impose any threats on data integrity). Issuance and verification of Authenticity MUST be located in Trust Zone II or III.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

Originator Authenticity: at minimum message exchange level end-to-end security MUST be provided (contributes to liability). Issuance and verification of Authenticity MUST be located in Trust Zone II or III.

Access Control: at least at minimum message exchange level end-to-end security MUST be provided (users do not alter medical data, therefore unauthorised access does not impose any threats on data integrity). Attribute provisioning and policy decision/enforcement must be located in Trust Zone II or III.

Non-repudiation of origin: node/country level end-to-end security is sufficient. Communication MAY terminate in Trust Zone I.

Non-repudiation of delivery: node/country level end-to-end security is sufficient. Communication MAY terminate in Trust Zone I.

End-2-end protection demands on the lifecycle and business levels must be covered by dedicated security services. End-2-end protection demands on the message exchange and node levels should be covered by Data Exchange Security Services.

Data Exchange Security Services MUST serve confidentiality (including mediation of entity authentication), communication liability (including non-repudiation and originator authenticity) and access control. This can be done by either implementing respective security mechanisms as part of the data exchange protocol or by securely exchanging security tokens through the data exchange protocol.

An analysis of the protection demand of the managed objects can now be done easily by reflecting the already mentioned core protection demands. E. g. a patient identifier has high protection demands on integrity and confidentiality (alteration might provide unauthorized access to another patient's data, disclosure might give information on which physician is treating the patient).

2.2.1.3.4 e1-REQ-1796 Data Exchange Security Services

The analysis of the data exchange security services and the underlying security mechanisms and security objects is organised according to the steps of the baseline security process as defined in the ISO/IEC-27001 standard.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.3.5 e1-REQ-1797 Scoping (IT Network)

The epSOS topology of epSOS-NCPs is a peer-to-peer network of autonomous application level gateways. Each gateway corresponds to a set of service endpoints which mediate requests into the national healthcare infrastructure. Data exchange security services provide message exchange end-to-end security between the sender and the receiver of a message which are both located on the application level (ISO layer 7). In the case of epSOS these are the epSOS-NCP gateways of Country A and Country B.

 epsOS <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.2.1.3.6 e1-REQ-1798 Analysis of Alternatives

2.2.1.3.6.1 e1-REQ-1803 Security on Different Layers of the OSI Reference Model

The OSI reference model defines an abstract model that describes the layered communication between systems over network protocols. It identifies different layers that use services of underlying layers and provide services to layers on top of them[ISO7498-1]. Message Protection (e.g. encryption) must be implemented at least on one of those layers. Which layer is appropriate highly depends on the identified security requirements.

The number of systems that can be bypassed/bridged by the security context is highly dependent on the layer that is chosen to protect the communication. Information is only protected up to the layer that the security protocol resides in. A processing of information by a protocol in a higher layer makes it necessary to unprotect (e.g. decrypt) the message, process it and protect it again. The security context is interrupted. It is no longer possible to speak of end-to-end security.

The next chapter will provide a detailed overview about specific security mechanisms and their advantages and disadvantages with regard to the layer that they are implemented in.

2.2.1.3.6.2 e1-REQ-1804 Mechanisms for realizing End-to-End Security

epsOS builds upon an architecture that is dominated by the exchange of SOAP messages over existing (public) networks. With regard to providing a secure message exchange, it is therefore necessary to identify and evaluate the mechanisms that are appropriate for a web service environment and that provide the requested level of end-to-end security.

The following widely adopted mechanisms will be part of the comparison:

IPsec (Layer 3)

Transport Layer Security (SSL/TLS) (Layer 4+)

SOAP Message Security / Web Service Security (Layer 7)

Application Based Security (Layer 7)

 <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.2.1.3.6.3 e1-REQ-1810 IPsec (Network Layer Security)

Layer / Description: IPsec is a composition of protocols that protects traffic on the network layer. Especially the Encapsulation Security Payload (ESP), the Authentication Header (AH) and the Internet Key Exchange (IKE) Protocols are suitable for providing protection with regard to most of the identified security objectives. [RFC4301].

Confidentiality Mechanisms: Confidentiality can be guaranteed by using security functions provided by the ESP protocol. [RFC4301]

Integrity Mechanisms: Integrity can be guaranteed by using security functions provided by the ESP or AH protocol. [RFC4301]

Authenticity Mechanisms: Authenticity can be realized by using the Internet Key Exchange Protocol. Many authentication methods including one based on public key cryptography and certificates are supported. [RFC4306]

Non-Repudiation Mechanisms: IPsec can secure the communication channel but not single SOAP messages as they are sent between web services implemented within the SPOT framework. In consequence the security objective of non-repudiation cannot be addressed.

Security Scope: The security context is restricted to communication on the network layer. Therefore only protocols and systems can be bridged that work on the same layer or below. (e.g. switches and routers) If information must be processed on higher layers of the protocol stack the security context must be terminated by unprotecting (e.g. decrypting) the information.

Advantages: IPsec is well understood and implemented by many software manufacturers. It can be implemented without affecting the source code of the application that relies on the provided security mechanisms. (Security by Declaration)

Drawbacks: IPsec offers no solution for addressing the security objective of non-repudiation. In addition it is not possible to authenticate endpoints on the level of single web services. Only authentication on the network service level is provided. The protocols underlying IPsec tend to be complex. This makes it hard to integrate them properly.

Relevant Standards: RFC4301, RFC4302, RFC4303, RFC4306, ... , PKIX

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.3.6.4 e1-REQ-1811 Transport Layer Security (SSL/TLS)

Layer / Description: The TLS protocol is integrated above the transport layer (Layer 4) and can secure TCP based communication. TLS consists of two layers: the TLS Record Protocol and the TLS Handshake Protocol.

Confidentiality Mechanisms: Confidentiality can be guaranteed by using symmetric encryption functions. (e.g. AES, DES, RC4, etc.) These functions are implemented by the TLS Record Protocol.

Integrity Mechanisms: Integrity is provided by a security service of the TLS Record Protocol. This service provides a keyed message authentication digest on the basis of MD5 or SHA.

Authenticity Mechanisms: The peer's identity can be authenticated using asymmetric or public key cryptography (e.g., RSA, DSS, etc.). This authentication can be made optional, but is generally required for at least one of the peers.

Non-Repudiation Mechanisms: TLS secures the information channel but not single messages. Digital signatures that might state non-repudiation are only used for authentication. [Gallop06] So there are no appropriate mechanisms in place for securing the communication in the context of this security objective.

Security Scope: Communication security can be provided on a relatively high level. Protocols and systems that work on lower levels (e.g. switches, routers, and proxies) can easily be bridged/tunneled. However, message processing on higher layers makes it necessary to terminate the security context and unprotect the transferred information. With TLS the security context will always be terminated by a network service that resides in an IT system. But especially in the case of web service communication it might be necessary to terminate the context directly at the web service endpoint.

Advantages: Transport Layer Security can easily be integrated for providing a secure communication between two peers. Most web service frameworks include this functionality by default. Because of this TLS security can be applied without changing the source code of the application relying on the protocol. (Security by Declaration)

Drawbacks: TLS offers no solution for addressing the security objective of non-repudiation. Only the information channel is secured but not single messages. Because of this it is almost impossible to prove, that a certain message has been sent. Furthermore only network services can be authenticated by using public key cryptography. An authentication of specific web service endpoints is not realizable. [Iacono08]

Relevant Standards: RFC2246, RFC4346, RFC5246, PKIX

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.3.6.5 e1-REQ-1812 SOAP Message Security / Web Service (Layer) Security (WSS)

Layer / Description: SOAP Message Security (Web Service Security) describes enhancements to SOAP messaging to provide message integrity and confidentiality. [WSS1.1] Based upon mechanisms described in [WSS1.1] several specifications and profiles have been published that refer to all of the security objectives identified in chapter 1.1.

Confidentiality Mechanisms: Message confidentiality leverages XML Encryption in conjunction with security tokens to keep portions of a SOAP message confidential. [WSS1.1]

Integrity Mechanisms: Message integrity is provided by XML Signature in conjunction with security tokens to ensure that modifications to messages can be detected. [WSS1.1]

Authenticity Mechanisms: Authentication is based on the evaluation of security tokens that are embedded into SOAP messages. Several different security token profiles have been specified. (e.g. username tokens, X.509 tokens etc.) [NIST07]

Non-Repudiation Mechanisms: Web service security is implemented on the application layer. This provides the possibilityto of auditing and evaluating specific message content that is relevant in the context of non-repudiation. For example the existence of a specific security token (e.g. X.509 tokens) and its usage in conjunction with the XML signature standard can provide the proof that a message was send by a specific subject. [NIST07]

Security Scope: Implementing security mechanisms on the SOAP message level provides the advantage that the security context spans above all systems and services that takes part in transmitting the message from its sender to its recipient. (e.g. routers, proxies, application level gateways) Even systems like intermediate web services that have to process certain parts of the SOAP message can do this without terminating the security context.

Advantages: Many of the current web service frameworks provide the possibility of enabling SOAP message security by configuring the runtime environment appropriately. (Declarative Security) This makes it relatively easy to address the security needs of certain web services. The implementation of security at the SOAP message level makes it possible to process parts of messages at intermediate nodes even without the need to terminate the security context.

Drawbacks: A comparison with other mechanisms like TLS shows that the integration of security on the SOAP message level is more expensive i with regard to performance. [Ekelhart07] The realization of security on the application level can only protect information that has its seeds on that level. Additional information generated after protecting the message (e.g. addressing information, routing information) won't be secured and can therefore be analyzed and/or compromised.

Relevant Standards: WS-Security, WS-SecurityPolicy, WS-Trust, WS-ReliableMessaging; WS-SecureConversation, WS-Federation, SAML, XACML, PKIX, XMLEnc, XMLDSig, XKMS. An overview and description of Web Service Security Standards is given in [SPOT_WSS].

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.2.1.3.6.6 e1-REQ-1813 Application Layer Security

Layer / Description: Message security is provided on the application layer (7) of the OSI reference model by protecting the message payload with the help of cryptographic functions.

Confidentiality Mechanisms: Confidentiality can be guaranteed by individually protecting the content/payload of a message. (e.g. with the help of cryptographic functions for information encryption)

Integrity Mechanisms: Integrity can be guaranteed by individually protecting the content/payload of a message. (e.g. with digital signatures)

Authenticity Mechanisms: Authenticity can be guaranteed by individually protecting the content/payload of a message. (e.g. with digital signatures that are based on certificates/keys corresponding to a specific subject)

Non-Repudiation Mechanisms: Non-repudiation can be guaranteed by individually protecting the content/payload of a message (e.g. with digital signatures that are based on certificates/keys corresponding to a specific subject) in conjunction with auditing mechanisms.

Security Scope: The scope of this security mechanism is really broad. Information can be secured across any system participating in the communication. (e.g. Proxies, Application Level Gateways, Web Services). Security can even be maintained while information is in storage.

Advantages: The implementation of security on the level of messages content provides the advantage that mechanisms can be integrated that are matching the specific needs of underlying application or data. Security mechanisms are not specific to data in transit. They can also be used to protect information in storage.

Drawbacks: Security mechanisms are specific to certain applications and can hardly be reused for other purposes. Security is often applied programmatically. This makes it necessary to change the source code of an application. If the integrated functionality is not based on common standards it's hard to evaluate if the integrated mechanism addresses relevant security objectives properly.

Relevant Standards: XMLEnc, XMLDSig, PKCS#7, PKIX, PGP

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

2.2.1.3.7 e1-REQ-1799 Evaluation of the Alternatives

The preceding sections described mechanisms that are able to protect communication on different layers of the OSI reference model. In this section they are analysed with respect to the epSOS requirements on the different security objectives.

2.2.1.3.7.1 e1-REQ-1805 Confidentiality

End-to-end message confidentiality can be provided by transport layer, message layer and application layer security mechanisms. The drawback of message and application layer mechanisms not protect addressing information is of no importance for epSOS because communication is always only epSOS-NCP-to-epSOS-NCP.

Comparison of pros/cons for confidentiality mechanisms

	IPSec (Network Layer)	SSL/TLS (Transport Layer)	SOAP/WS Security	Application Layer
Appropriateness of provided mechanisms	-	+	+	+
Matching of terminating Trust Zones	-	-	+	+

2.2.1.3.7.2 e1-REQ-1806 Integrity

Even though the integrity of medical data has to be addressed by specific means, a violation of the integrity of other arguments (e. g. a patient identifier in a query) might lead to unauthorized disclosure of medical data. Therefore the protection demand on the integrity of message exchange is high; communications ends must be located in Trust Zone I or II. End-to-end message integrity can be provided by network layer, transport layer, message layer and application layer security mechanisms.

 epSOS <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Comparison of pros/cons for integrity mechanisms

	IPSec (Network Layer)	SSL/TLS (Transport Layer)	SOAP/WS Security	Application Layer
Appropriateness of provided mechanisms	+	+	+	+
Matching of terminating Trust Zones	-	-	+	+

2.2.1.3.7.3 e1-REQ-1807 Authenticity

If end-to-end authenticity is required, mechanisms on the transport, message and application layer are appropriate. But as the epSOS security policy links certain guarantees with the signature of the epSOS-NCP it is important that epSOS-NCP authenticity is precise, which means that a epSOS-NCP gateway MUST have its own and exclusive service certificate and the only matching termination points are epSOS-NCPs. This cannot be realised by IPSec or TLS, which rely on node certificates.

Comparison of pros/cons for authenticity mechanisms

	IPSec (Network Layer)	SSL/TLS (Transport Layer)	SOAP/WS Security	Application Layer
Appropriateness of provided mechanisms	-	-	+	+
Matching of terminating Trust Zones	-	-	+	+

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.3.7.4 e1-REQ-1808 Liability (Non-repudiation)

Non-repudiation can only be provided by mechanisms on the message and application (message payload) level. Based on certain requirements it must be decided which mechanism is appropriate. The realization of this security objective on the application level provides the advantage of keeping non-repudiation information beyond message transfer (e.g. in storage) without the necessity of protocolling whole SOAP messages.

Comparison of pros/cons for non-repudiation mechanisms

	IPSec (Network Layer)	SSL/TLS (Transport Layer)	SOAP/WSS Security	Application Layer
Appropriateness of provided mechanisms	-	-	+	+
Matching of terminating Trust Zones	-	+	+	+

2.2.1.3.7.5 e1-REQ-1800 Conclusions

Security mechanisms on the message layer (WSS) as well as on the application layer are appropriate to provide complete end-to-end communication security for each of the identified security objectives. While SOAP/WSS security terminates at Trust Zone II, application layer mechanisms can even be tied into Trust Zone III.

In general it is easier to implement SOAP message security (web service security) by just declaring the specific security needs inside the web service framework (declarative security). In contrast application based mechanisms make it necessary to adjust the source code (programmatic security).

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.1.3.8 e1-REQ-1801 Option Presentation

Taking into account that end-to-end node communication at MS country level, due to public network interfaces, must in every case be protected by TLS/SSL protocol, and under the constraints that in each MS domain communication between Trust Zone I and Trust Zone II should be protected by dedicated VPN, two possible solutions are analyzed also considering operational and economical factors.

Comparison of pros/cons for (WS-*enc/sig +TLS) vs (WS-*sig +TLS+VPN)

Option	WS-*	TLS	VPN	Confident.	Non-rep.	Maturity	Complexity	Performance	Segr. of Duty
"A"	enc/sig	enc	-	+	+	-	-	-	-
"B"	sig	enc	enc	+	+	+/-	+/-	-	+

The main advantage of option "A" is related to the lack of confidentiality protection needs between Trust Zone I and Trust Zone II communication. This fact may greatly reduce the complexity of security conformity tests of each NCP implementation.

On the other hand, option "B" presents advantages in performance, in development complexity and it is a more mature solution. Moreover the segregation of duty in operational environments is easier to achieve, because the VPN is on network level which is frequently administered by different staff from the Webservice infrastructure.

2.2.1.3.9 e1-REQ-1802 Option Selection

From the security point of view both options "A" and "B" guarantee an adequate level of protection. WP3.4 SHOULD analyse the options from 5.8.

As the above mentioned solutions just apply to the message payload level, the following additional mechanisms MUST be provided:

To reach the required level of liability, audit trails MUST be written to accompany the reliable transmission of data.

To support the security objectives of access control and HCP authenticity, respective security tokens MUST be exchanged securely as part of the SOAP Security Header.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.1.3.9.1 e1-REQ-1809 TLS version to be adopted

Three versions of TLS protocol are available on the market, with a different level of diffusion:

TLS 1.0 rfc2246, TLS 1.0 using SHA-1 algorithm, is the most widely adopted.

TLS 1.1 rfc4346, TLS 1.1 was updated from the previous version 1.0, adding, as major significant difference, the protection against Cipher block chaining (CBC) attacks.

TLS 1.2 rfc5246, TLS 1.2 significantly improves the previous versions, the cryptographic algorithm and provides support for 256 bit Hash functions (SHA-2).

Having in mind the timeframe of epSOS pilot phase, to be concluded within 2012, TLS with SHA-1 may be considered as sufficient . Therefore the indication given is to adopt the TLS version more widely implemented (TLS 1.0 RFC 2246).

2.2.1.3.10 e1-REQ-1828 Non-repudiation

rewrite D3.7.2-S2 §7

- a) consider renaming to accountability
- b) reduce to normative text

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.2.1.4 e1-FLD-146 Computational Dimension

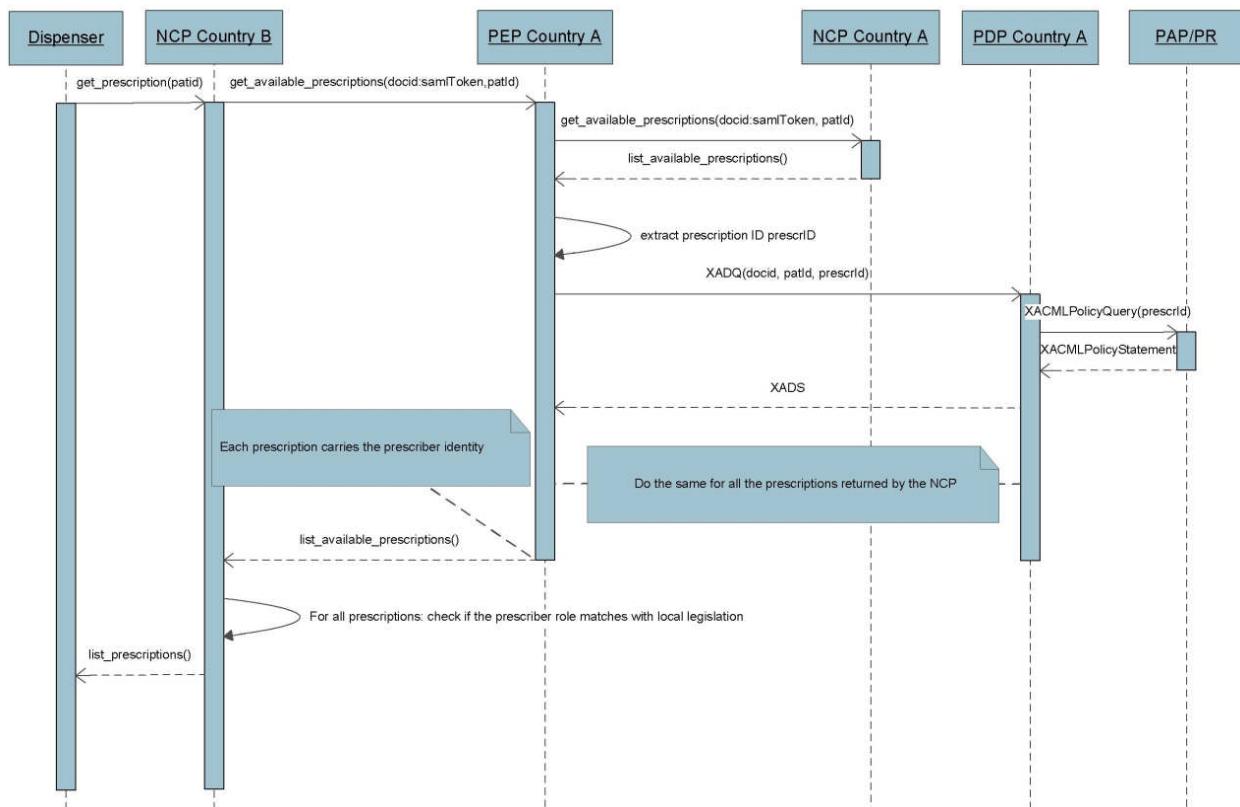
2.2.1.4.1 e1-REQ-4981 Process Access Control with epSOS Use Cases

Related to e1-REQ-4977 EpSOS-Req#3.7.04 (Access control)

Related to e1-REQ-4978 EpSOS-Req#3.7.05 (Access control, privilege management and HP authorization)

Related to e1-REQ-4979 NCP-Req#3.7.04 (Access Control)

Related to e1-REQ-4447 REQ 3.6.38 County A decides in emergency cases



By making reference to the figure above, the process is analyzed. The figure depicts the ePrescription use case. The message SHALL be conformant with OASIS SAML 2.0 Profile of XACML:

The `get_prescription(docId:samlToken, patId:String)` message is sent by a dispenser in order to obtain all the available prescriptions for the patient. This message contains the identity and attributes for the HCP (i.e. in case of doctor, `docId`, as SAML token) and the

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

identity of the patient, *patId*, according to WP3.4 and WP3.6 definitions. This server-side flow is sent through NCP-B to NCP-A.

NCP-A validates the SAML assertion (methods defined in WP3.6, WP3.4).

NCP-A obtains the prescriptions for the given patient ID and extracts a list of prescription ids (*prescriId*) to be used as XACML Resources for authorization decisions.

For each prescription id contained in the list, NCP-A requests an authorization decision from the ACS actors (PEP, PDP, PAP/PR) for the *prescriId* and the identity contained in the *docId* SAML token to be used as request *Subject*.

PEP in Country A creates a *XACMLAuthzDecisionQuery* SAML request according to for the PDP in Country A. In this case, the PEP plays the role of implicit CH. The XACML request inside SHALL map the attributes contained in the SAML authentication assertion. The *<Subject>* element of the request MUST have an attribute *urn:oasis:names:tc:xacml:1.0:subject:subject-id* as the SAML assertion subject. The patient MUST be inside the request. The epSOS defined role MUST be contained in the *urn:oasis:names:tc:xspa:1.0:subject:role*.

If the policy is not cached, PDP in Country A performs a *XACMLPolicyQuery* to the PAP/PR in Country A for obtaining the policy governing the given prescription ID.

Once the PDP in Country A gets the policy, it performs the policy decision and replies to the PEP with the *XACMLAuthzDecisionStatement*.

A deny-based PEP enforces the decision from the PDP and informs the NCP-A.

After all access control decisions have been made, the NCP-A creates the “filtered” list of available prescriptions. Each prescription MUST contain the prescriber functional role in the prescriber identity as defined by epSOS.

The list of available prescriptions is sent back to the NCP-B.

For each prescription, the NCP-B enforces local legislation duties using a similar mechanism. It checks if the prescriber role matches with the permitted roles in the local legislation, according to the Example 3 of the document *The epSOS Trusted Domain(s), Consolidation of Concepts*.

A similar scenario applies for the Patient Summary use case, where the transaction is the *get_available_summary()*.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.2 e1-REQ-4602 REQ 3.3.17 HP-B authentication at NCP-B

Related to e1-REQ-1981 HP-B Identification and Authentication

Health professional of country B may either authenticate at NCP-B or NCP-B should confirm a previously done authentication by the health professional to a trusted Identity Provider in country B.

2.2.2.1 e1-REQ-4834 REQ 3.3.17.1 National Connector guarantees HP authentication claims

The National Connector (NC) of NCP-B MUST guarantee the correctness of the HP authentication claims that are assigned to the National Interface (NI).

2.2.2.2 e1-REQ-4835 REQ 3.3.17.2 National Connector guarantees document access by authenticated HP

The National Connector of NCP-B MUST guarantee that any CDA documents obtained from the National Interface are forwarded only to the HP that was authenticated as issuer of the request.

2.2.3 e1-REQ-4608 REQ 3.3.23 Emergency Access through NCPs

Related to e1-REQ-4446 REQ 3.6.37 Processes for emergency cases

Access without consent in the vital interests of the patient, where the patient cannot give consent, shall follow the same process as the standard access to a PS, although the local consent confirmation should be replaced by a consent override notification checked by health professional at PoC-B.

As a result, NCP-A rules MAY be more relaxed than the standard procedure for accessing a PS (e.g. less/no consent) in order to grant access.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.2.4 e1-REQ-4618 REQ 3.3.26 Communication of identified exceptions

Related to e1-REQ-4847 Error Handling

There are NCP-related exceptions, which MUST be defined.

There are national infrastructure related exceptions, which SHOULD be covered by the national infrastructures.

For each exceptional solution, the epSOS exception handling specification MUST provide guidance stating

if it MUST be communicated among gateways or

if it MUST, SHOULD or MAY be handled solely within the affected national infrastructure

2.2.5 e1-REQ-4619 REQ 3.3.27 Feedback in case of identified exceptions

Related to e1-REQ-4851 Information messages and warnings

epSOS system MUST provide all system user and system partners (i.e. HP, NCP and National Infrastructures) with appropriate feedback, even if the transaction failed.

2.2.6 e1-REQ-4620 REQ 3.3.28 National helpdesk as part of feedback system

An error feedback system must be established, including the support of a national helpdesk.

A hierarchy of error messages (3 classes) should be established which is easily understandable to the HP user, making clear when the user should abort the system:

Class I: *Try-again*, if it is a temporary error-producing situation (e.g. service not available),

Class II: *user-centric advice*, what went wrong (e.g. failed identification),

Class III: *call to higher instance* as something fundamental went wrong (e.g. national hotline). It is not mandatory for each PN to support such a "hotline", but it is mandatory to specify a national contact if a fatal error must be propagated.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.2.7 e1-REQ-4621 REQ 3.3.29 Error-message severity codes

Related to e1-REQ-4847 Error Handling

The decision to propagate an error-message must be related to its code severity. There are five levels of severity defined in the list below which should be considered.

It should be mandatory to propagate the "CRITICAL" Level. Every bilateral agreement between two PN can define to give each of the severity levels a dedicated action.

Severity Codes:

Debug: Only for internal use (technical experts)

Info: Only for internal use

Warning: Some flaws, but the transaction is performed

Error: The transaction may or may not succeed

CRITICAL: Critical failure, transaction must be cancelled

2.2.8 e1-REQ-4622 REQ 3.3.30 Logging of errors

Related to e1-REQ-4868 Audit Trail Considerations by NCP-A & NCP-B

Related to e1-REQ-4862 Audit Trail to be generated by NCP-B

Every failure MUST be logged in the Audit Trail.

2.2.8.1 e1-TXT-726 Note

It might be sufficient to just use a general error code with participants, date and time. But regarding to the severity code, it can also be most important to log as much information as possible.

2.2.9 e1-REQ-1951 Traits Handshake central function

Related to e1-REQ-4606 REQ 3.3.21 Common epSOS resources

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

NCP-A and NCP-B should be able to agree on the identity traits that have to be provided by country B in order to identify a patient. Information on which traits are required for which country MAY be coded within a static client-side configuration. It is the responsibility of each country B client/portal to keep the configuration up to date.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.2.10 e1-REQ-1950 Taxonomy for the epSOS pivot format central function

Related to e1-REQ-4606 REQ 3.3.21 Common epSOS resources

Related to e1-REQ-4987 MTC Creation

Related to e1-REQ-4986 Semantic Content Workflow

Related to e1-REQ-4989 Transcoding from national code system to the MVC

Related to e1-REQ-4990 Transcoding from the MVC to national code systems

The Taxonomy central function serves as a library for all existing and valid epSOS pivot formats and all relevant schemas. This information should be robust most of the time and not to be changed. Therefore this information can be duplicated into each NCP. This should also be relevant for later performance issues. Each NCP must hold a copy of the taxonomy from a known URL (e.g. www.wpsos.eu/taxon/) where each NCPs can retrieve a copy. It is the responsibility of each PN to keep the configuration up to date for the NCP.

2.2.11 e1-REQ-5298 Common Data Sources for NCP Operation

Related to e1-REQ-4606 REQ 3.3.21 Common epSOS resources

Related to e1-REQ-4833 NCP Configuration Manager Interface and Functionality

Common data which MUST be in the same state within every NCP SHALL consist of following classes, distribution type is indicated within brackets ():

- a) Master ValueSets Catalog (MVC) (1)
- b) List of participating PN (“PN-List”) (1)
- c) each member state's Master Translation Catalog (MTC) (2)
- d) Trust anchors (3)
- e) End point addresses, VPN, NCP, IdP and HCP certificates (in TSL) (3)
- f) MS policies & documents (3)
 - 1. (Patient) information paper
 - 2. Confirmation requirement policies
 - 3. HCP allowed roles
 - 4. NCP PS eP data hiding disclaimer

This shared data should be centrally managed in order to avoid inconsistencies and version conflicts in the epSOS network.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.11.1 e1-TXT-886 Note

Common data in the context of epSOS technical infrastructure has following distribution types:

- (1) identical for all PNN participating in epSOS
- (2) specific for each NCP but derived from a common source
- (3) specific for each NCP and public to all other NCPs

2.2.12 e1-REQ-4987 MTC Creation

Related to e1-REQ-1950 Taxonomy for the epSOS pivot format central function

Mapping from a national schema to the pivot documents schema is **out of the scope** of epSOS.

There are 1-3 tasks for each PN to perform to be able to make their national translations and transcodings in accordance with the requirement to deliver the data needed in the epSOS pivot documents.

The first task is mandatory for all PNs. The second and third tasks are only required if an PN uses another code systems than the ones selected in the epSOS Reference Terminology to represent the data in a value set and if they wish to see the data in their own systems and not only wrapped in an additional pdf file.

2.2.12.1 e1-REQ-4988 Translation of the MVC

Each PN in the epSOS project MUST complete a translation of all the concepts in the MVC to be able to read a file from Country A in Country B national language.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.2.12.2 e1-REQ-4989 Transcoding from national code system to the MVC

Related to e1-REQ-1950 Taxonomy for the epSOS pivot format central function

If a PN uses another code system nationally than the one selected to represent the data in the value sets of MVC the PN must transcode/map from the national code systems to the code systems in the MVC to be able to deliver the data required in the pivot documents.

2.2.12.3 e1-REQ-4990 Transcoding from the MVC to national code systems

Related to e1-REQ-1950 Taxonomy for the epSOS pivot format central function

If an PN wishes to see a file from Country A in the PNs national systems and uses other code systems than the ones in the MVC then the PN must transcode/map from the code systems in the MVC to national code systems to be able to see a file from Country A in the PNs national systems.

2.2.13 e1-REQ-1949 Trusted Certificates

Related to e1-REQ-4606 REQ 3.3.21 Common epSOS resources

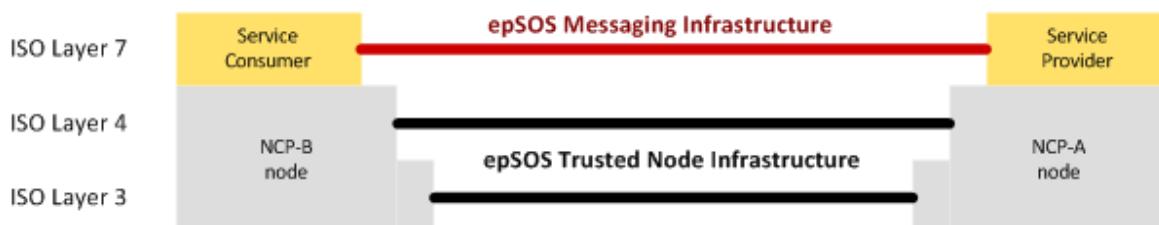
Related to e1-REQ-4833 NCP Configuration Manager Interface and Functionality

Certificate services are PN issues. Technical trust in country A is established by acknowledging the certificates that were announced by country B and vice versa after legal trust confirmed. Certificates from different certificate service providers should be used per communication layer (VPN, TLS, WS-Security).

2.2.14 e1-REQ-4885 Trusted Node Infrastructure

Related to e1-REQ-1879 Trusted Node Infrastructure

epSOS service providers and consumers use the epSOS messaging infrastructure to exchange request and response messages among each other. The message infrastructure builds upon the epSOS communication infrastructure that connects the epSOS network of trusted nodes as depicted in the figure below.



The epSOS trusted node infrastructure MUST implement the core epSOS security services that

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

ensure the confidentiality of medical data transmission and the availability and authenticity of epSOS services:

virtual private network (VPN) on top of the public internet,
message encryption (TLS) and integrity protection, and
mutual NCP authentication.

2.2.14.1 e1-TXT-769 Note

It must be noted that only NCPs acting as epSOS service providers and consumers are part of the epSOS trusted node infrastructure. Points of Care within country B or national data registries/repositories in country A have to be connected to the epSOS trusted nodes by means that respect the epSOS end-to-end privacy, security and data protection requirements. See epSOS SecurityPolicy and epSOS D3.7.2 for details.

2.2.15 e1-REQ-1948 National Contact Point Discovery Table

Related to e1-REQ-4606 REQ 3.3.21 Common epSOS resources

Related to e1-REQ-4882 Service Discovery

The Locate central function is a simple NCP Routing Table which facilitates the connections between two NCPs. This information is encoded in a NCP configuration file which is specified by D3.4.2. Each NCP MUST hold a copy of the configuration files of all the other NCPs.

2.2.15.1 e1-TXT-768 Note

This service is independent of the form of distribution (e.g; centrally maintained, replicated or locally maintained copies) and can be made available as an XML-document.

2.2.16 e1-REQ-4882 Service Discovery

Related to e1-REQ-1948 National Contact Point Discovery Table

Related to e1-REQ-4833 NCP Configuration Manager Interface and Functionality

For the 2011/2012 epSOS pilots service discovery and location will be based on static location tables (see epSOS D3.3.2, epSOS HLDD).

Each NCP MUST describe its service addresses and certificates in a centrally managed location table that complies to the epSOS *Trusted Service List* (TSL) format as specified in e1-REQ-4883.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Each NCP MUST hold a copy of the other NCP's location tables as part of its internal configuration. How the respective files are distributed and managed is out of scope.

The framing conditions of the processes for the maintenance and distribution of centrally managed data are given in epSOS D3.7.2. The definition of these processes and the application of safeguards for preserving the authenticity and integrity of this data is subject to the epSOS operations guidelines.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

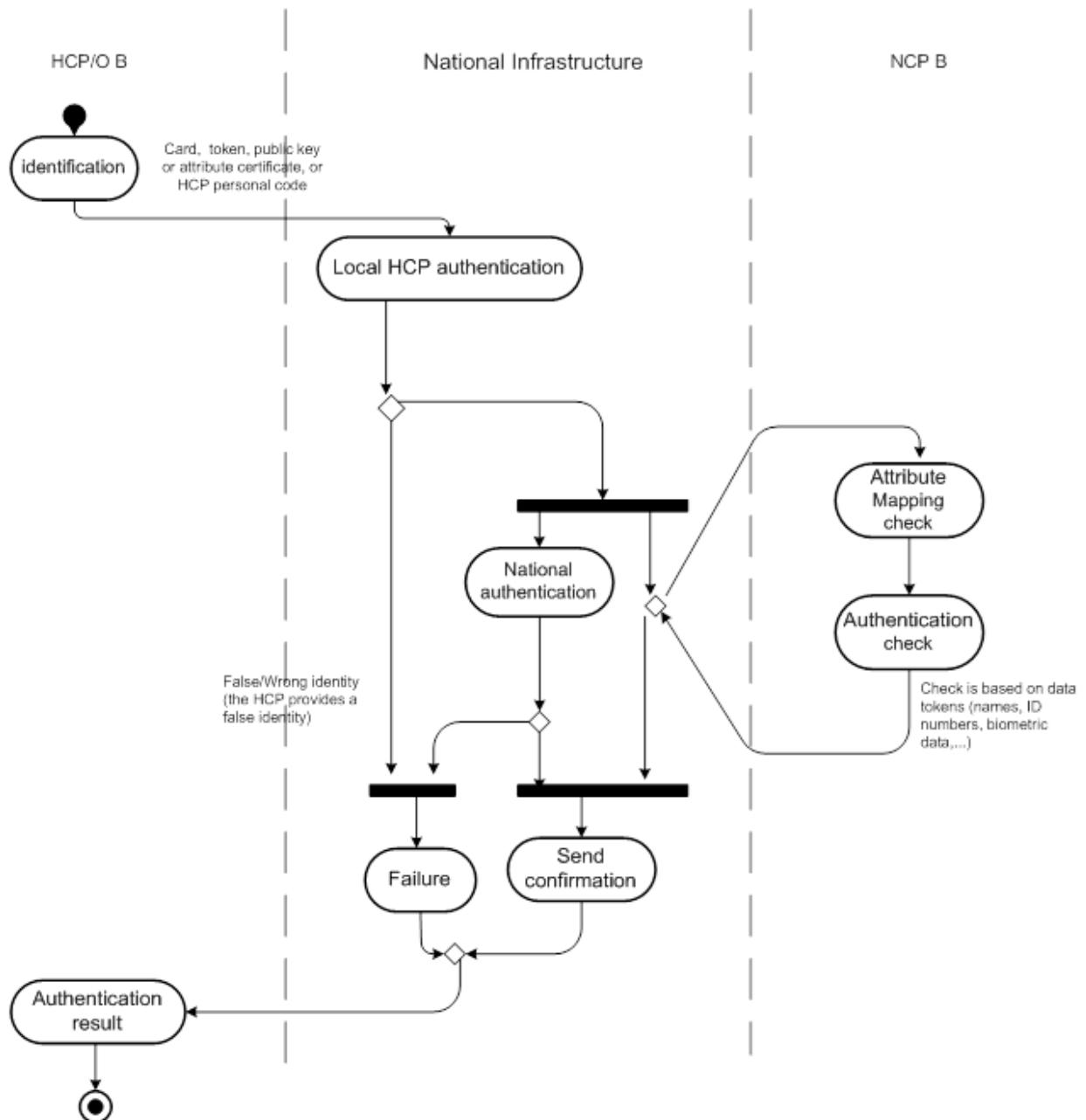
2.2.17 e1-REQ-1721 Description of the flow of control

HP Identification & Authentication

At the beginning of the process, identification procedure initiated by the HP is insufficient to face the threat of a false HP identity. The authentication can solve this problem. HP provides identification information and NCP verifies the formal correctness of provided information through the attribute mapping check operation. The proclaimed identity and genuine identity of the HP will be validated during the authentication check step of the initial protocol. The identification/authentication result will be finally sent back to the HP(O) B.

NB: HP(O) and Infrastructure A/B parts are PN concern. The processes involved are presented as guidelines with no mandatory requirement.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013



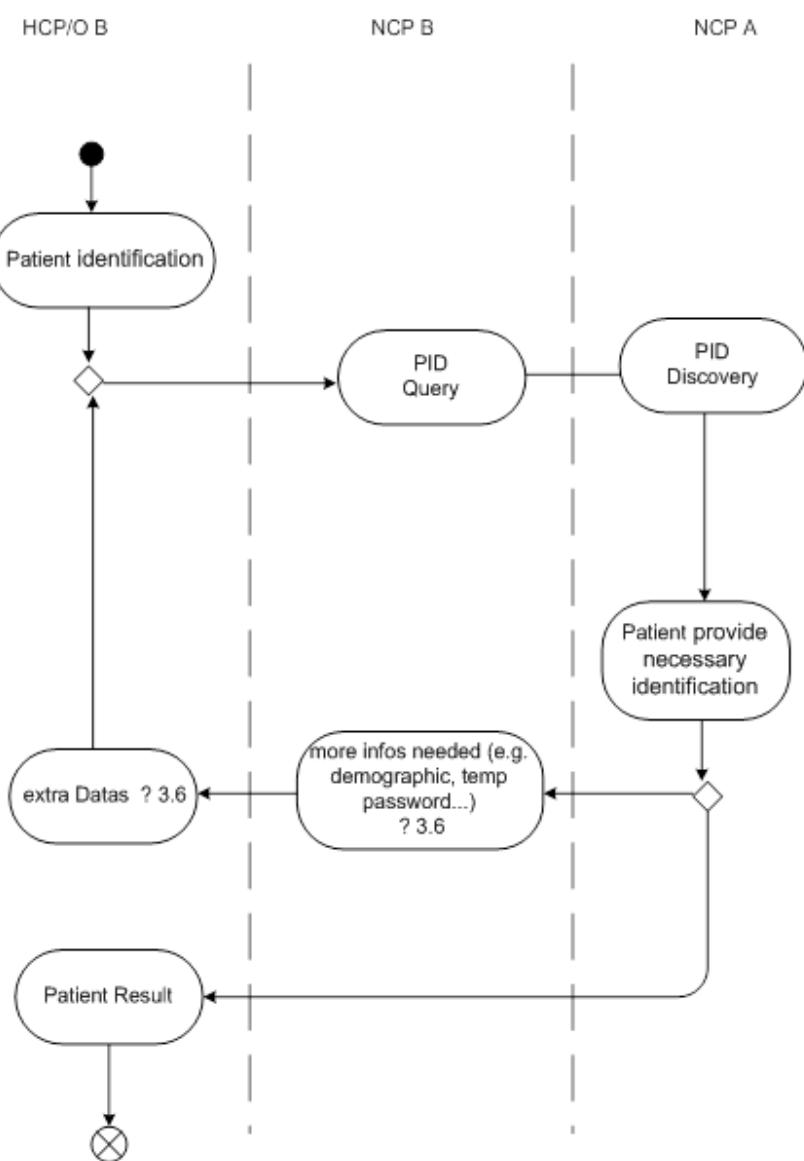
	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

Patient Identification

When a patient needs a health service (health care, ePrescription) in a foreign country B two sub-cases are considered:

The HP receives necessary identification information and is able to identify the patient.
 Patient identification information is not enough according to country A regulations and requires additional data (e.g. temporary password). PN can use TAN (Temporary Access Number) for patient authentication. It is not a mandatory field and PN are free to choose traits for their citizens.

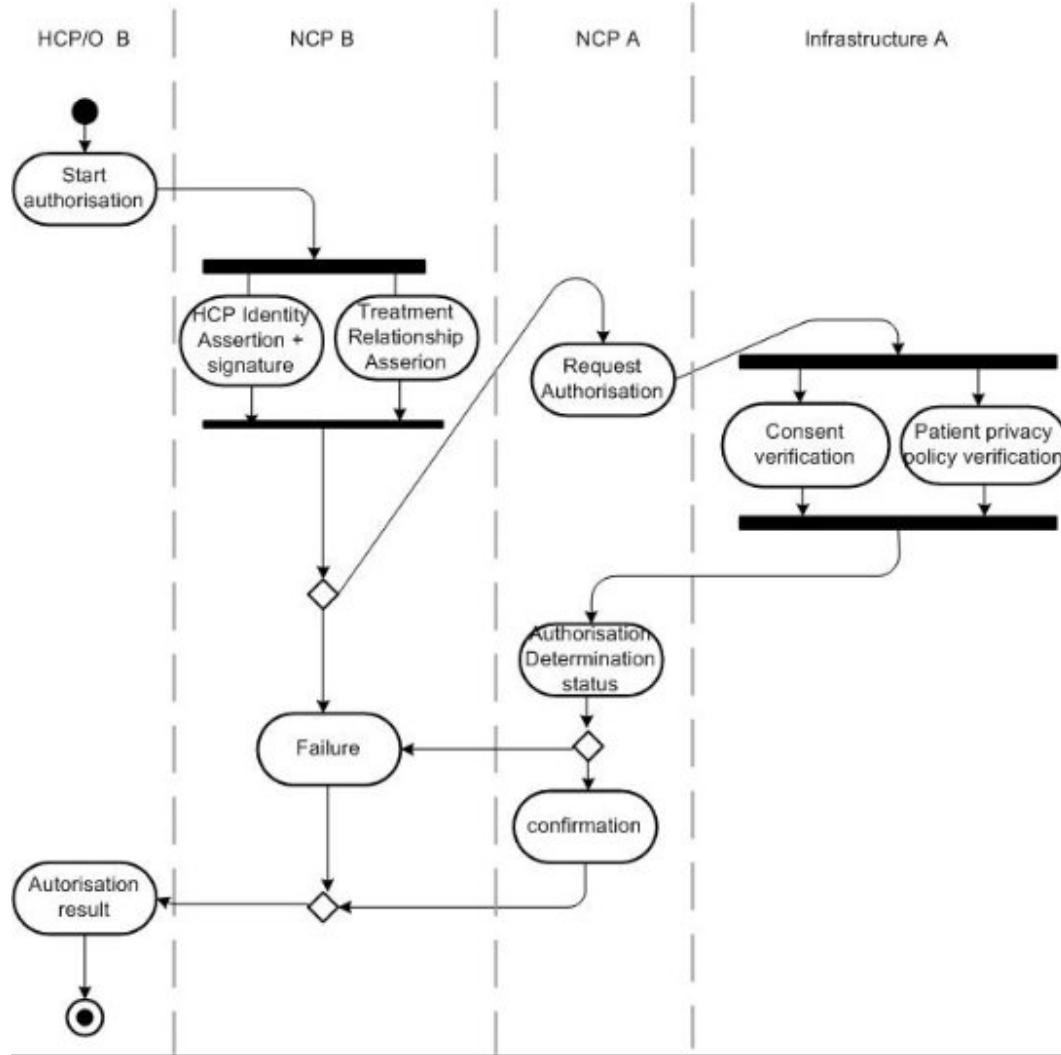
Only Identification of a patient by a HP in country B is represented in this schema.



 Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3	Date: 31/01/2013

NB: HP(O) and Infrastructure A/B parts are PN concern. The processes involving them are presented as guidelines with no mandatory requirement.

Treatment Relationship Confirmation



A treatment relationship confirmation issue by HP(O) informs the patient that his medical data will be accessed. The patient MUST be informed to give his consent for this operation. The identity of HP(O) with a signature is also encapsulated in the message. The signature of NCP-B MUST be recognized by NCP-A. When the message reaches country A, the Patient privacy policies state who can benefit the right to access his/her data's. A patient has to state his consent for the exchange of his/her medical data in accordance with the patient consent policy in country A. According to the type of data that needs to be accessed, country A determines the status as a result of consent and policy verification in country A. In addition to the Actors role,

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

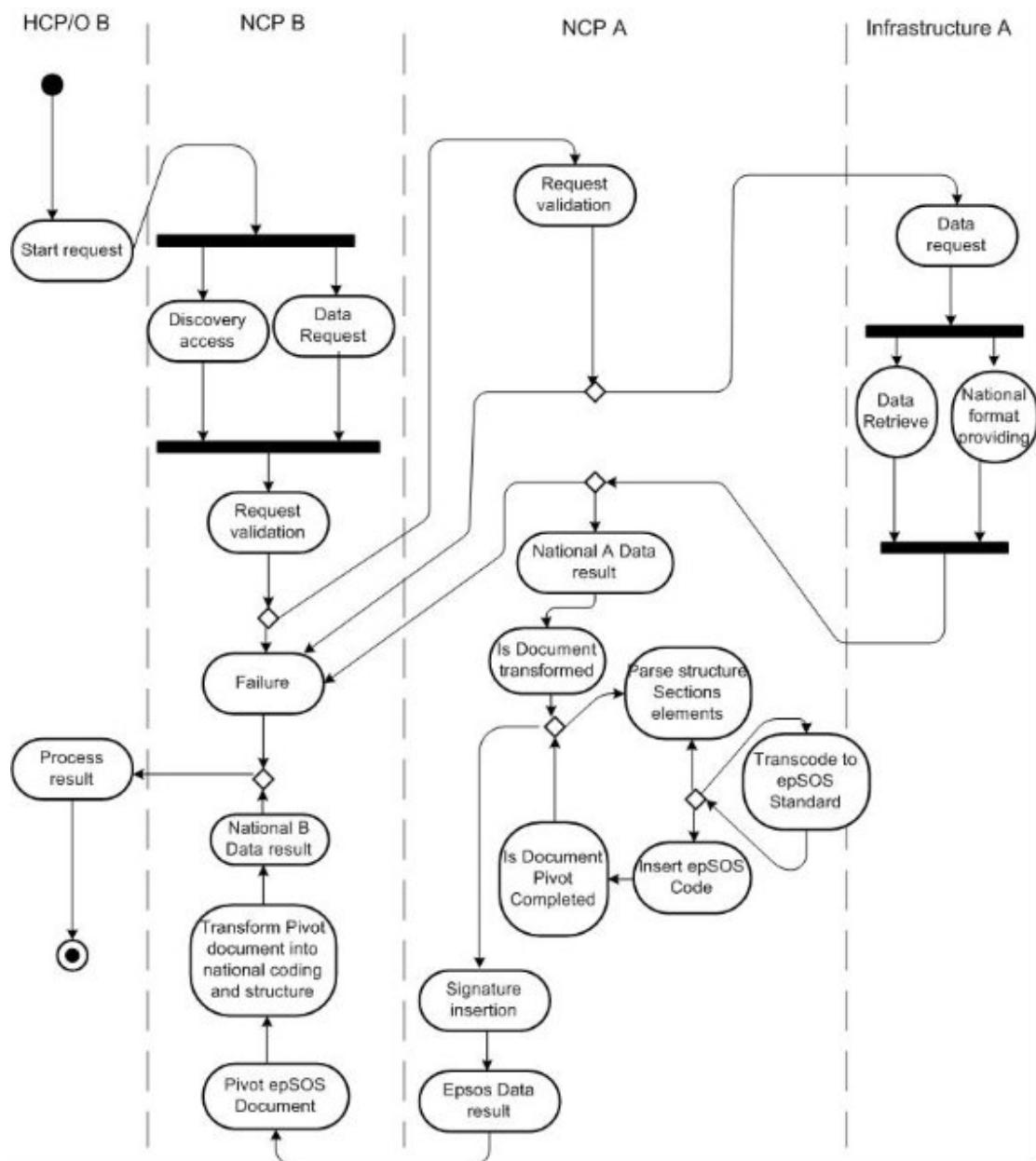
confirmation or rejection depends on the type of data.

The confirmation assertion as defined in D3.4.1 will be part of D3.4.2 (some extensions may be intro-introduced). It will be mandatory for country B to provide this assertion, but country A MAY decide to ignore it. An attribute that will be used for indicating an emergency access scenario (already defined by D3.4.1) will be included in the TRC assertion.

NB: HP(O) and Infrastructure A/B parts are PN concern. The processes involved are presented as guidelines, PN states if they deliver Medical Data for the patient.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0 Date: 31/01/2013
D5.2.3		

Data Retrieval



The data retrieval process returns medical data under National Format. The steps to follow in order to achieve the semantic transformation process are provided here:

The medical document is retrieved by NCP-A. The document MAY be digitally signed.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The nominal process is the following: NCP-A verifies the validity of the signature and checks the authenticity and integrity of the document. In case of a successful verification NCP-A signs the document.

The document is transformed into the epSOS pivot format by NCP-A (format defined in D3.5.2, CDA)

The original document is provided as a PDF or rendered as PDF and enveloped.

NCP-A MAY create a detached signature over the pivot document, the PDF document and the original signature. If PDF is provided by the system, there is no need for NCP-A to sign it. This attests that: authenticity and integrity were checked and the pivot document is a transformation of the original document.

Both documents (original and pivot) and signatures are sent to NCP-B.

NCP-B transforms the pivot document into country B native format and handles it over to the HP.

Transformation and data validation are specific to each country (various national formats in use). The retrieval task is a national concern and in any case Country A is responsible to provide the result or the exception/failure outcome back to the requestor (Country B).

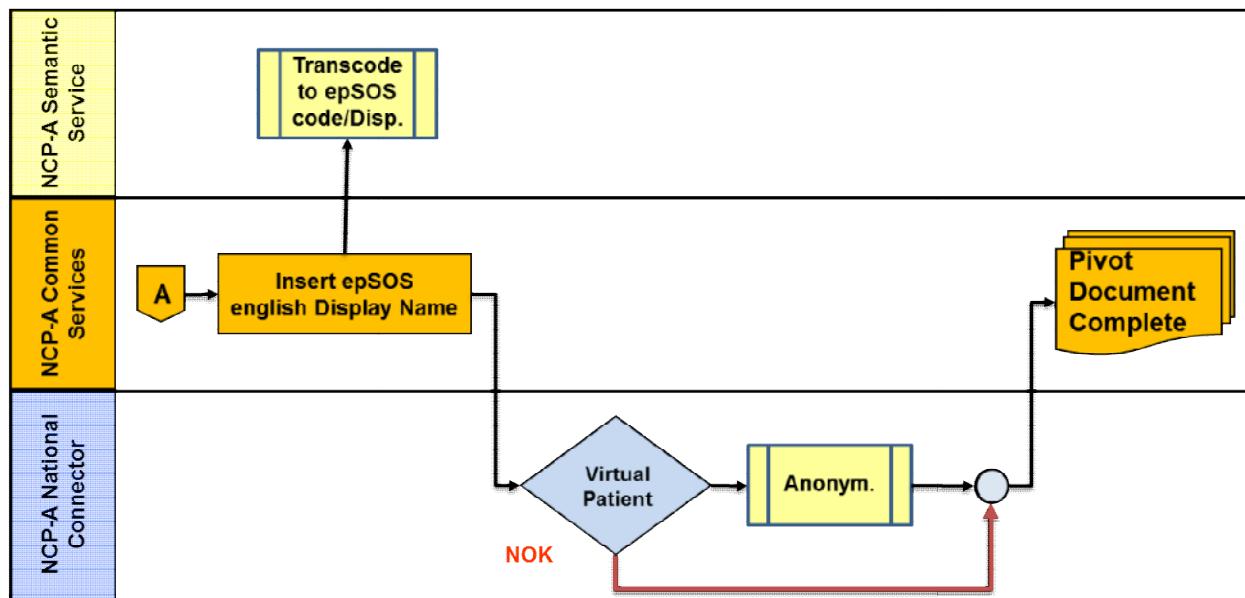
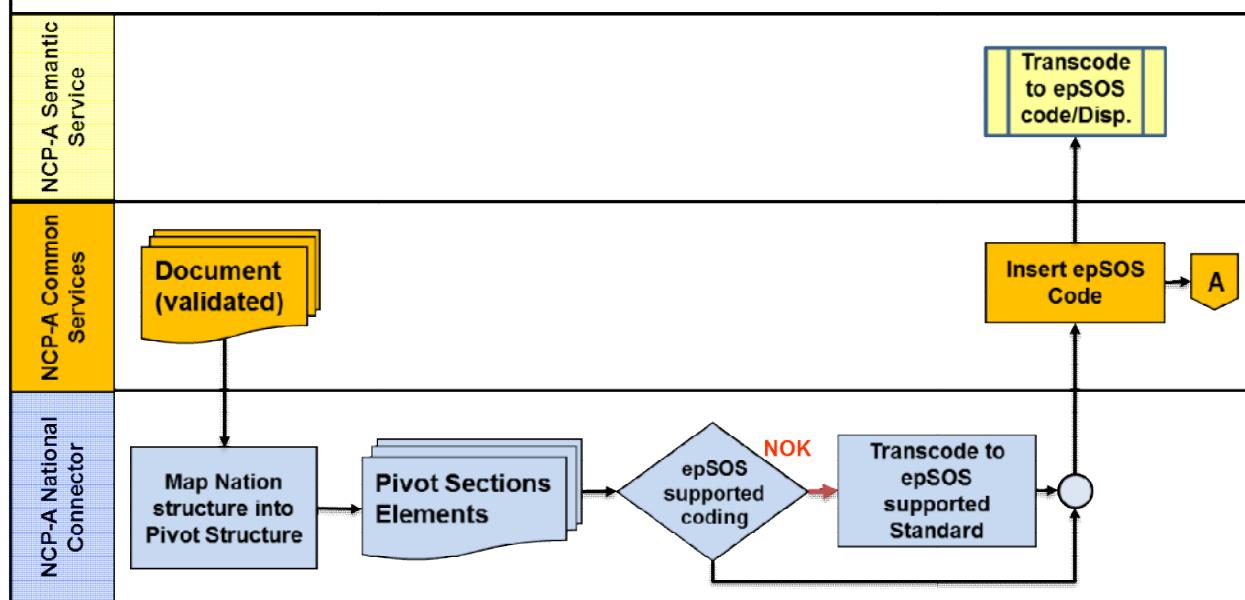
As proposed by WP3.5, the sequence diagrams for the transformation / transcoding operations at NCP-A and NCP-B are described in the two figures below (source WP3.5):

NOTE : To avoid multiple dispensation for the same prescription, pharmacist retrieves ePs and dispenses. A policy will be defined that a pharmacist always MUST first retrieve the current list of available prescriptions before he can dispense anything. This is in line with the Industry Team proposition that it is up to the pharmacist to manage its stock and that state machine and eP lifecycle management is to be done in Country A. D3.1.2 will be revised accordingly (no E2E-sessions, HP-B policy).

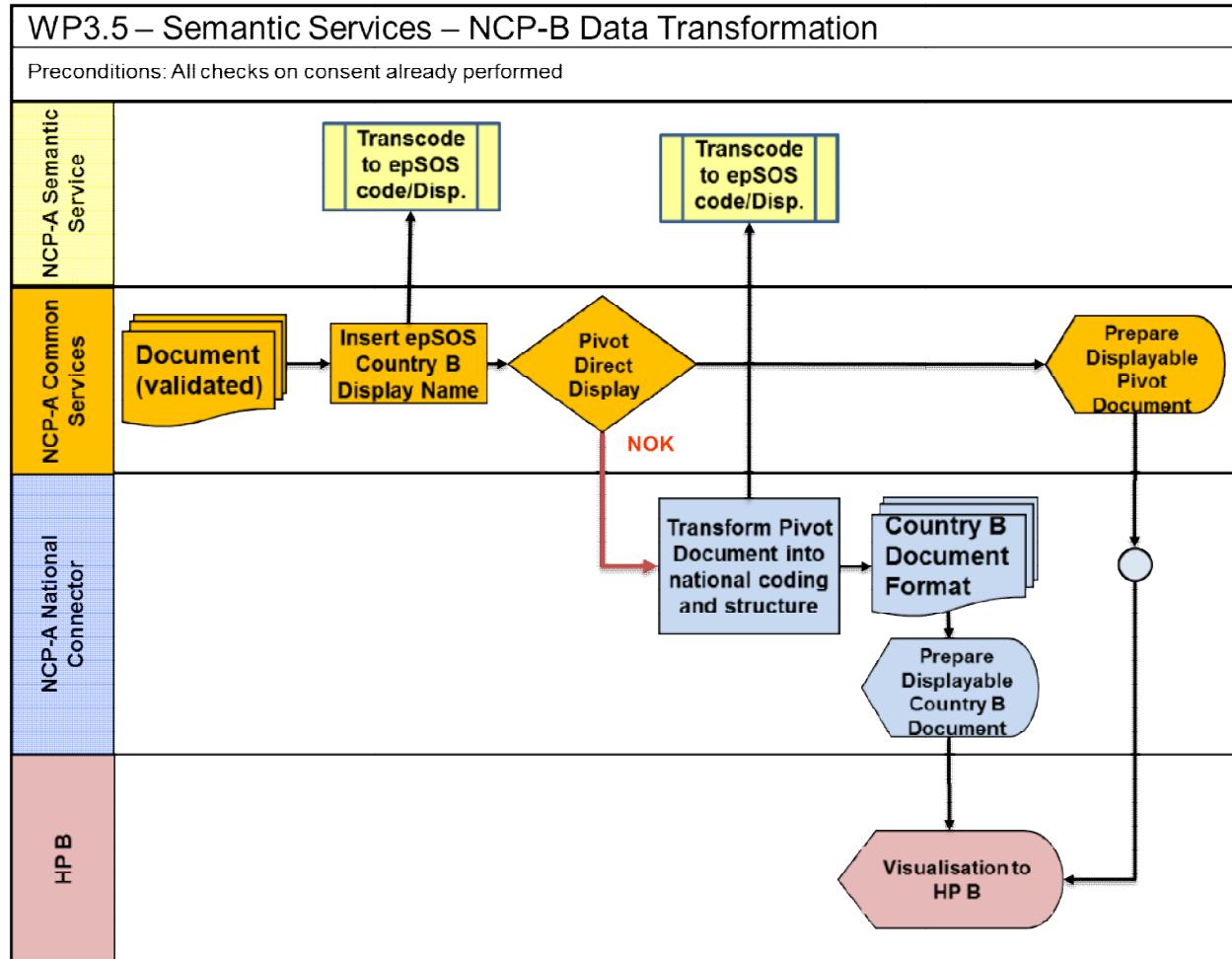
	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

WP3.5 – Semantic Services – NCP-A Data Transformation

Preconditions: Nation A Data retrieved for the identified patient. All checks on consent already performed



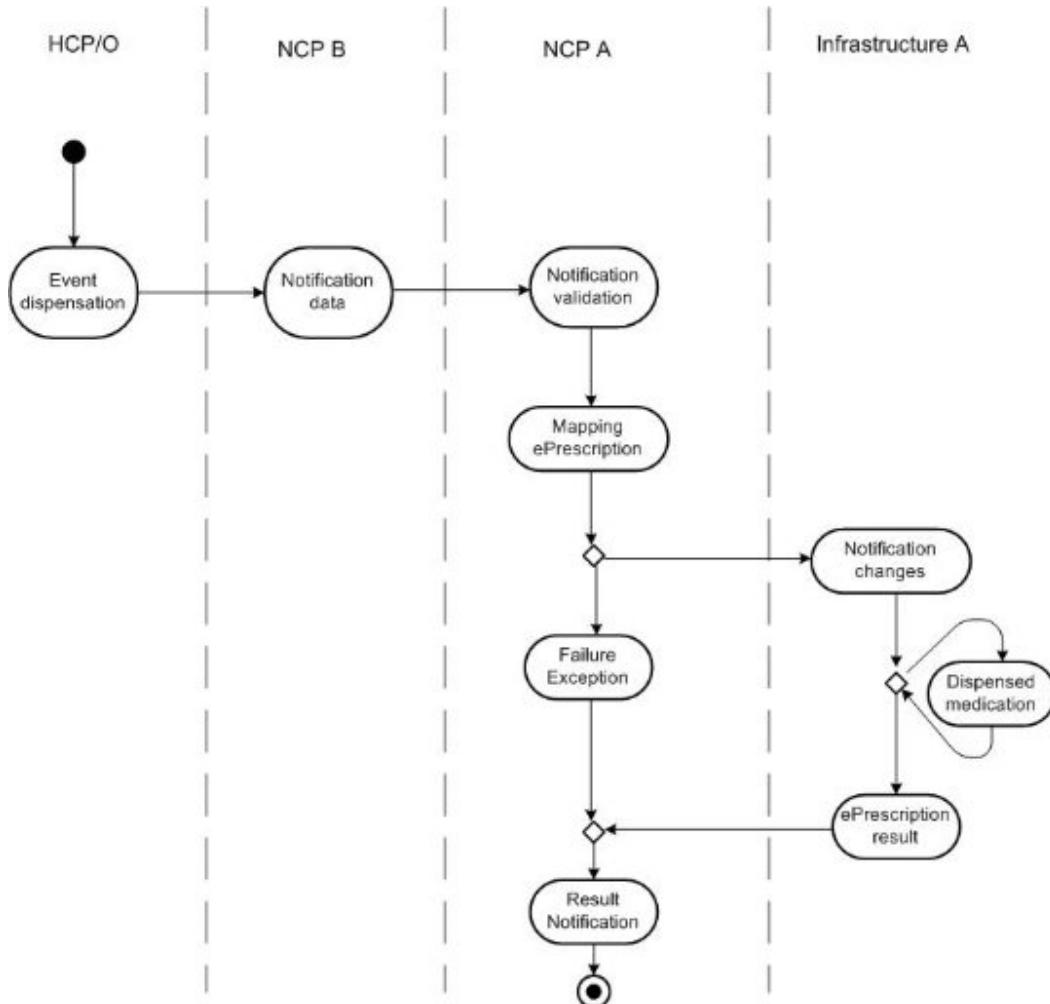
	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



NB: National Connector and Infrastructure A/B parts are PN concern. The processes involving them are presented as guidelines with no mandatory requirement.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

Send Notification



Notification occurs when an event is triggered (e.g. a dispensed medicine in country B). The notification object is then transported from B to A and verified. Because partial dispensation of a medicine is possible, Country A must provide a way to update the ePrescription.

Unless the Notification result has been sent, no more dispense for the same ePrescription will succeed the validation process in country A. NCP-A gives its ok ("Notification validation"); NCP-B does not wait for eP result (no return arrow from A); NCP-A assures updates ("Mapping ePrescription").

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.2.18 e1-REQ-4836 NCP-B Internet Front-End

HPs acting as a PoC in a country B shall have the option to use the web portal to access epSOS services.

2.2.18.1 e1-REQ-4837 System Overview

The NCP-B Front-End SHOULD be based on the enterprise java (Java EE) referable reduced version containing the necessary part for Java Servlet Pages/Java Server Faces (JSP/JSF) execution (recommendation), but this can be changed with justification. It MUST support the Services for Patient Identification (ID), Patient Consent (PC), patient Summary (PS), ePrescription (eP) and eDispensing (eD); consuming the first four Services and publishing/sending/pushing the latter.

2.2.18.2 e1-REQ-4838 Portal Adaptor

The interface with/to the NCP MUST go through the NCP Portal Adapter, that decouples the country-B web portal and the core NCP.

2.2.18.2.1 e1-TXT-733 Note

Communication to and from the Front-End to NCP need the Portal Adapter, because the National Connector is unknown (national specific), and therefore to have a common/unique interface between the two systems, a portal specific adapter is needed.

2.2.19 e1-REQ-4841 General Considerations for Service Operations

Related to e1-REQ-4831 Consent time frame validity

Related to e1-REQ-4844 epSOS ConsentService Service Interface & Functional Specification

Related to e1-REQ-4843 epSOS DispensationService Service Interface & Functional Specification

Related to e1-REQ-4845 epSOS IdentificationService Service Interface & Functional Specification

Related to e1-REQ-4842 epSOS OrderService Service Interface & Functional Specification

Related to e1-REQ-4840 epSOS PatientService Service Interface & Functional Specification

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

In order to successfully operate the epSOS services, the following preconditions MUST be met:

The service consumer MUST be able to locate the service provider. The respective end point addresses and certificates MUST be provided through a Trusted Service List. Up-to-date copies of all service providing NCP's Trusted Service Lists MUST be available to the service consumer.

A secure channel MUST have been established between service consumer and service provider nodes.

The service provider MUST be able to verify the authenticity of the service consumer and vice versa. This requires that service consumer and service provider only make use of digital certificates that can be verified by the counterpart.

The requesting HP MUST have been authenticated in the country of care (see D3.6.2 for details on HP authentication). The service provider MUST be able to verify the attesting HCP identity assertion. NCP signature certificate MUST be used for attesting the successful authentication of an HP.

Failures during a service's operation or faulty conditions for using a service MUST be handled. Part of this fault handling is that a respective audit trail entry MUST be written at all NCPs who are aware of the fault. See e1-REQ-4860 for details.

Further general requirements for secure and privacy-aware operations that MUST be considered are defined in D3.7.2 and epSOS SecurityPolicy.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.2.20 e1-REQ-4847 Error Handling

Related to e1-REQ-4851 Information messages and warnings

Related to e1-REQ-4618 REQ 3.3.26 Communication of identified exceptions

Related to e1-REQ-4621 REQ 3.3.29 Error-message severity codes

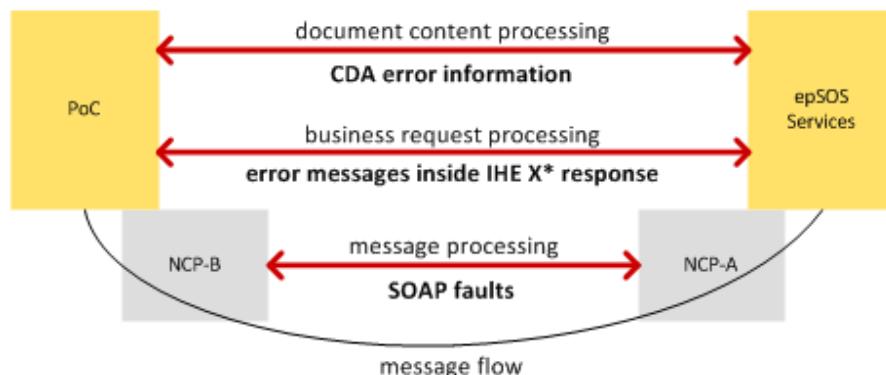
Related to e1-REQ-4860 Exception Handling

Failures during operation execution can be of different kinds; e. g. they MAY be caused by syntactic mismatches, insufficient access rights, country-A component failures or protocol failures. epSOS should make use of three different error reporting mechanisms in order to allow for a better handling of errors on the appropriate level of abstraction:

SOAP Faults

Error messages in the SOAP response body

Error messages related to the creation of the document content



2.2.20.1 e1-REQ-4848 SOAP Faults

Related to e1-REQ-4860 Exception Handling

The standard SOAP fault mechanism MUST be used for failures that originate in the encoding of the SOAP message or the contents of the SOAP header.

2.2.20.1.1 e1-TXT-736 Note

It is assumed that the respective errors are discovered during the processing of the message at the epSOS communication tier of the NCP-A and that they mainly address failures that originate at NCP-B. Typical examples of such errors are missing security token or usage of undefined attributes within security token.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.2.20.2 e1-REQ-4849 Error Messages in the SOAP response body

Error reporting mechanisms of the business level protocol (e. g. XCF) SHOULD be used for failures that are discovered during the business-level processing of security token and SOAP body elements. These errors may as well be discovered during policy enforcement at the NCP as during the processing of the request within the national infrastructure. These errors SHOULD be reported to the HP in country B as it is assumed that either the HP or the patient MAY be able to take action to successfully re-issue the request. Business level error messages and their proposed processing are provided in the “response message” sections of the epSOS service specifications.

2.2.20.2.1 e1-TXT-737 Note

The failure usually either originates at the Point of Care in country B or at the national infrastructure in country A. Typical examples of such errors are missing consents and temporary component failures in country A.

2.2.20.3 e1-REQ-4850 Error messages related to the creation of the document content

There may be cases where failure to access certain systems within a national infrastructure may result in some elements of clinical information missing (e.g. in a patient summary). These clinical content errors should be conveyed within the document content.

2.2.20.3.1 e1-TXT-738 Note

The SOAP body transactions and SOAP header were exchanged without errors at the lower two levels.

2.2.21 e1-REQ-4851 Information messages and warnings

Related to e1-REQ-4619 REQ 3.3.27 Feedback in case of identified exceptions

Related to e1-REQ-4847 Error Handling

epSOS implements medical data sharing among different legal and technical environments. This might lead to scenarios where the NCP at the patient's country of affiliation MAY wish to send further information on the data collection procedure or on the source environment together with the data to the HP in the country of care. Even an uncertain state of a request's fulfillment – e.g. NCP was not able to access all relevant data sources – MUST be reported to the data consumer in order to provide a correct semantic context for the provided data.

To allow for this exchange of context information, all ebXML based epSOS messages MUST provide the ability to include an `<rs:RegistryErrorList/>` element (with an success indicator) for transmitting information and warnings together with provided medical data. Warnings that only affect the contents of a single document SHOULD be reported in an explicit

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

clinical statement within that document.

Service specific context information is provided in the “Errors and Warnings” sections of the epSOS service specifications.

2.2.22 e1-FLD-169 Information Dimension

2.2.23 e1-FLD-149 Computational Dimension

2.2.23.1 e1-REQ-4833 NCP Configuration Manager Interface and Functionality

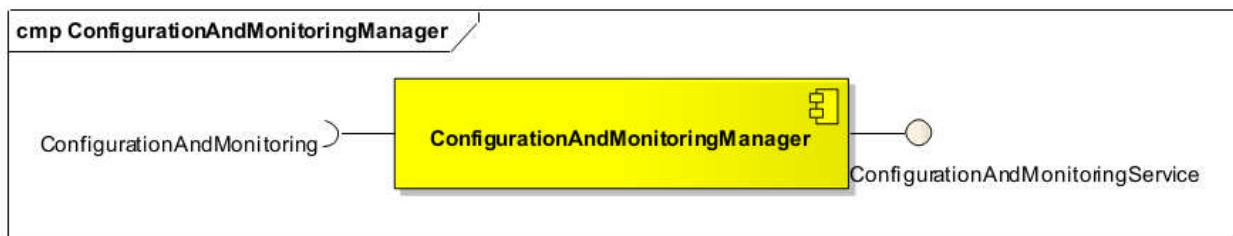
Related to e1-REQ-4882 Service Discovery

Related to e1-REQ-1949 Trusted Certificates

Related to e1-REQ-4883 epSOS Trusted Service List

Related to e1-REQ-5298 Common Data Sources for NCP Operation

This subcomponent should be responsible for analyzing the audit trail and, based on a configurable way easy to maintain for administrator. Alert should prevent possible abuses (such as excessive requests issued from a HP or a patient is queried from more than one country at a time).



Configuration and Monitoring Manager is responsible for keeping epSOS configuration, at the application boot start, the synchronicity with central epSOS repository (e.g. NCP routing and taxonomy access). The monitoring should be able to detect fraud. It is the responsibility of each NCP to keep the configuration up to date.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

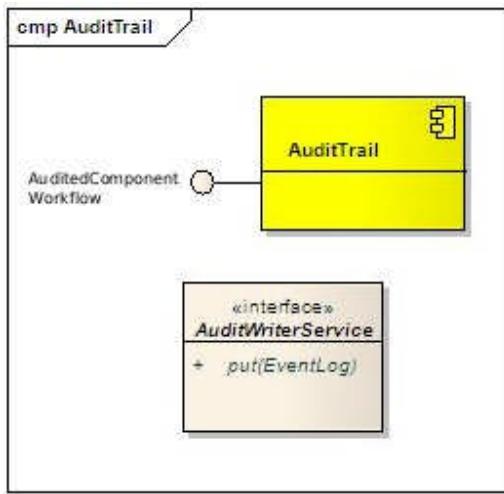
2.2.23.2 e1-REQ-4636 NCP Audit Trail Interface and Functionality

Related to e1-REQ-4960 Audit and Accounting

Related to e1-REQ-1835 epSOS Audit Trail Common Specification

This internal component is designed to implement the Audit Trail objectives. This component provides interfaces for the Audit Trail Service acting as service point, in order to keep track of events to be logged.

This AuditTrail component is responsible for receiving an EventLog message in an IHE ATNA-compatible way.



The AuditTrail accepts audit trail entries in an ATNA-compatible way, encapsulated in the Event Log. This REQ does not address detail for the storage procedure of the audit records.

The Audit Trail function is considered to be sufficient for data non repudiation and traceability, if a failure occurs.

2.2.23.2.1 e1-TXT-773 Note

See WP 3.8 for further details concerning implementation options.

2.3 e1-FLD-33 Implementable Perspective

2.3.1 e1-FLD-163 Information Dimension

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.1 e1-REQ-1883 epSOS Common Message Format

Related to e1-REQ-4945 epSOS Consent Service Protocol Requirements

Related to e1-REQ-4915 epSOS Dispensation Service Protocol Requirements

Related to e1-REQ-4872 epSOS Identification Service Protocol Requirements

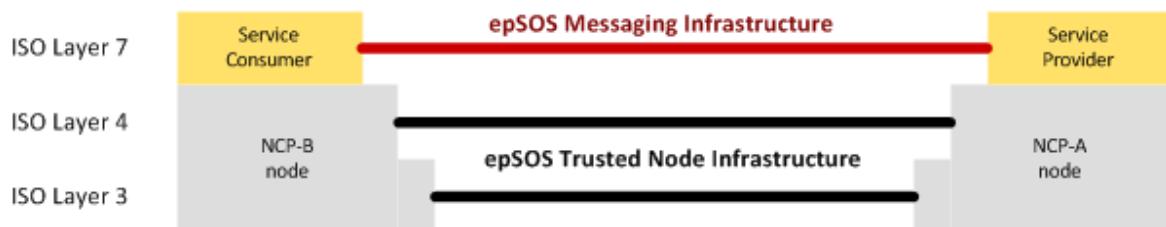
Related to e1-REQ-4905 epSOS Order Service Protocol Requirements

Related to e1-REQ-4888 epSOS Patient Service Protocol Requirements

The epSOS Common Message Format defines the structure and characteristics of the messages exchanged through epSOS and establishes the preconditions for successful communication. The epSOS Common Message Format describes only the structure of messages as they flow between service consumers and service providers. Messages within NCP's or national infrastructures may use any format desired, and need to be translated to the epSOS Common Message Format before transmission to another NCP.

2.3.1.1.1 e1-TXT-754 Note

epSOS service providers and consumers use the epSOS messaging infrastructure to exchange request and response messages among each other. The message infrastructure builds upon the epSOS communication infrastructure that connects the epSOS network of trusted nodes as depicted in the figure below.



The epSOS messaging infrastructure provides mechanisms for the implementation of the derived epSOS security services (e. g. non-repudiation and access control) and for the standardised enveloping of data and documents:

transmission of authenticated HP attributes,

common message format, and

signature on message elements for auditing and brokering of document authenticity claims.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.3.1.1.2 e1-REQ-1884 Transport Layer Profile

All messages MUST be sent over HTTP 1.1 connections that are layered on top of the epSOS trusted node infrastructure (see e1-REQ-1879).

2.3.1.1.3 e1-REQ-1885 Message Layer Profile

The epSOS Common Message Format is a SOAP 1.2, W3C SOAP 1.2 message contained as the body of an HTTP 1.1, RFC 2616 message.

All messages MUST be SOAP Envelopes with an XML payload in the SOAP Body. Optional binary data MUST be carried as Base 64 encoded octets within the XML payload if not otherwise stated for the respective operations. Request messages MUST be sent using an HTTP POST, response messages are carried over the backchannel, i.e. the HTTP response.

The encoding of the containing XML document MUST be set to UTF-8 [1].

All epSOS SOAP messages MUST comply with the WS-I Basic Profile 1.1[2] WSI BP 1.1.

All epSOS SOAP messages MUST comply with the WS-I Basic Security Profile 1.1 WSI SBP 1.1.

[1] UTF-8 is more efficient than UTF-16 for European languages. Older encodings such as ISO-8859-x do not cover all languages in a single encoding, and will only pose interoperability problems. UTF-8 is the default in XML, and coverage is a requirement of the XML specification.

[2] While WSI Basic profile 1.1 does not formally support SOAP 1.2, it takes into consideration SOAP 1.2 by having requirements which are specifically for compatibility with SOAP 1.2. IHE and epSOS plan to consider adoption of WS-I BP 2.0 WSI BP 2.0 as soon as it is approved by WSI.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.3.1.1.4 e1-REQ-1886 XML Message Schema Format

All epSOS SOAP message MUST be described in a WSDL 1.1 W3C WSDL 1.1 Service Description.

All WSDL type definitions MUST be in XML Schema format. One Schema must be provided for the request message, and one for the response message.

For better maintainability, an XML Schema import or include statement in the WSDL file SHOULD be used, so the XML Schema can be maintained and reused as a separate entity. If the XML Schema is small, and reuse is not expected, the entire Schema MAY be specified in the WSDL types section (especially in the case of RPC-style transactions where one or a few parameters of rather simple types are used).

2.3.1.1.5 e1-REQ-1887 SOAP Binding

For all messages a SOAP 1.2 HTTP Binding MUST be provided in the WSDL.

All SOAP Bindings in the WSDL MUST specify style="document".

All SOAP Bindings in the WSDL MUST specify use="literal".

The naming of the messages MUST be as defined for the used standard.

The "soapenv:mustUnderstand="1"" attribute MUST be set as defined for the used standard.

2.3.1.1.6 e1-REQ-1888 Embedding of Security Token

Each SOAP message MUST include a <wsse:Security> section within the SOAP header.

2.3.1.1.7 e1-REQ-1890 SAML Assertions

SAML assertions are contained within the <wsse:Security> section of the SOAP header. The HCP Identity Assertion always takes the role of a Supporting Token.

The saml:Advice element MUST be used to define the linkage between the two assertions (see e1-REQ-1909). Both assertions MUST have been issued for the same subject. The relying party MUST verify the correct linkage of the SAML assertions and the match of the <Subject> elements' contents.

2.3.1.1.8 e1-TXT-752 Note

Request messages are safeguarded by up to two SAML assertions that attest the authenticity of the user and the existence of a treatment relationship.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.1.9 e1-REQ-4884 Message Signature

Related to e1-REQ-4877 Cryptographic Keys and Algorithms

To preserve the integrity and authenticity of a message and to attest the NCP origin of the message, elements of each message MAY be signed by the protection token. If WS SecurityPolicy is used, a signed elements assertion MUST be used to refer to the message parts to be signed [1].

The following table defines which token MUST be used as protection token and which elements of the message MUST be covered by the signature.

	Request Message	Response Message
Protection Token	X.509 Token of NCP-B	X.509 Token of NCP-A
Signed Elements	/Envelope/Body /Envelope/Header/Security/Assertion	/Envelope/Body

Signatures MUST be placed within a XML-Signature compliant <ds:Signature/> element inside the SOAP security header. The recommendations given in section 8 of OASIS WS-Security 1.1 SHOULD be considered. In addition the following constraints apply:

Signature Parameter	Usage Convention
CanonicalizationMethod	SHOULD be "http://www.w3.org/2001/10/xml-exc-c14n#"
Transformation	Exclusive XML canonicalization SHOULD be used (http://www.w3.org/2001/10/xml-exc-c14n# , acc. W3C XMLDSig and W3C XML-EXC 1.0). As inclusive namespaces other prefixes than the ones defined in e1-REQ-4874 MUST NOT be used.
SignatureMethod	The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see e1-REQ-4877). For signing message elements the signature method " http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 " or " http://www.w3.org/2000/09/xmldsig#rsa-sha1 " SHOULD be used. A country MAY reject signatures that use SHA-1 for digesting.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

DigestMethod	<p>The hash algorithm MUST comply with the epSOS recommendations on algorithms and key lengths (see e1-REQ-4877). For signing message elements the digest method "http://www.w3.org/2000/09/xmldsig#sha1" http://www.w3.org/2001/04/xmlenc#sha256 SHOULD be used. A country MAY reject SHA-1 digests.</p>
KeyInfo	This element MUST contain a wsse:SecurityTokenReference element which references the protection token.

[1] Only in cases where the framework does not allow for multiple XPath expressions, a signed parts assertion SHOULD be used.

2.3.1.10 e1-REQ-1889 Processing of SOAP Messages

Related to e1-REQ-1234 Processing of SOAP Messages

A sending service consumer SHOULD add SOAP Message Headers in the order in which the receiving service provider is expected to process them.

A receiving service provider MUST not rely on a specific order of SOAP Message Headers for correct processing.

A receiving service provider MAY rely on a specific order of SOAP Message Headers for faster processing.

2.3.1.2 e1-REQ-4883 epSOS Trusted Service List

Related to e1-REQ-4930 epSOS Consent Service Message Specification

Related to e1-REQ-4914 epSOS Dispensation Service Message Specification

Related to e1-REQ-4852 epSOS Identification Service Message Specification

Related to e1-REQ-4903 epSOS Order Service Message Specification

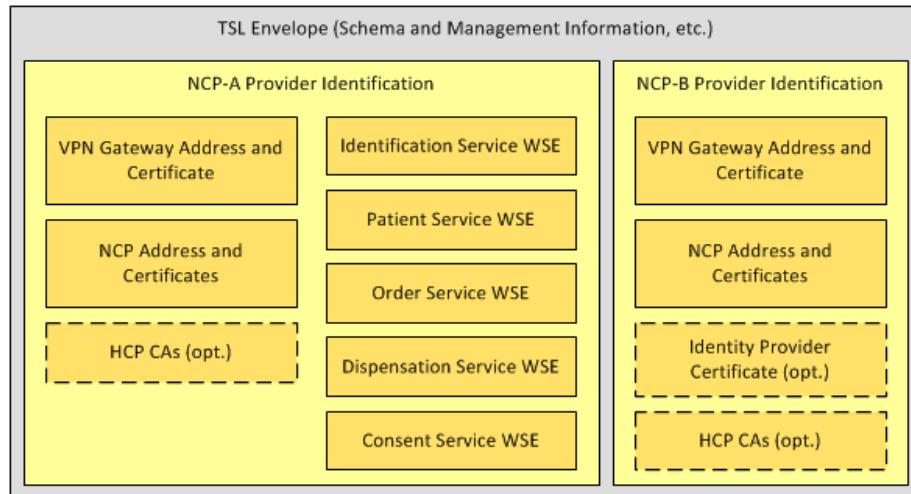
Related to e1-REQ-4886 epSOS Patient Service Message Specification

Related to e1-REQ-4833 NCP Configuration Manager Interface and Functionality

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

epSOS NCP Service Status Lists (NSLs) are encoded as ETSI Trust-service Status Lists acc to ETSI TS 102 231.

The following figure shows how the ETSI TSL structure is used to provide information on epSOS services.



epSOS NCP-Service Status Lists MUST be encoded in XML format according to Appendix B of ETSI TS 102 231. An additional human readable format SHOULD be made available in PDF/A format.

The following requirements define the application of ETSI TS 102 231 for encoding epSOS NCP-Service Status Lists.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

2.3.1.2.1 e1-REQ-1893 TSL Envelope

The fields for the TSL Tag, TSL scheme information and TSL Signature MUST be used as follows for encoding epSOS NSLs. The top-level body element MUST be `<tsl:TrustServiceStatusList/>`.

TSL Element	Opt	Usage Convention
@TSLTag	R	MUST be “ http://uri.etsi.org/02231 ”
@ID	O	SHOULD be “NCPConfiguration-Countrycode” (for the use of country codes see e1-REQ-4878)
SchemeInformation	R	This section provides information about the scheme operator. The scheme operator is responsible for publishing the epSOS NCP Service Status List and guarantees its authenticity and integrity. Unless not stated otherwise in the epSOS framework agreement, the role of the scheme operator MUST be taken by a national authority (e.g. the ministry of health).
TSLVersionIdentifier	R	MUST be “3”
TSLSequenceNumber	R	MUST be used acc. to ETSI TS 102 231. The sequence number MUST NOT be reset for different epSOS piloting phases.
TSLType	R	MUST be “ http://uri.etsi.org/TrstSvc/TSLType/generic ”
SchemeOperatorName	R	Name of the national authority that acts as the epSOS NSL scheme operator. The operator name MUST be provided in local language. It SHOULD additionally be provided in English.
SchemeOperatorAddress	R	Address of the national authority that acts as the epSOS NSL scheme operator. The operator address MUST be provided in national language. It SHOULD additionally be provided in English.
SchemeName	R	MUST be “NCP-Service Status List: <i>Countryname (Countrycode)</i> ” (for the use of country codes see e1-REQ-4878). The scheme name MUST be provided in

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

			national language and MAY additionally be provided in English.
	SchemeInformationURI	R	SHOULD refer to the epSOS Security Policy and the epSOS framework agreement.
	StatusDeterminationApproach	R	MUST be used acc. to ETSI TS 102 231. For epSOS pilot phase 1 epSOS NSL with a status of "passive" MAY be used by NCPs. From epSOS pilot phase 2 on only approved epSOS NSL (status = "active") MUST be considered.
	SchemeTypeCommunityRules	R	MUST be "http://www.epsos.eu"
	SchemeTerritory	R	MUST be the country code of the country that operates the NCP. (for the use of country codes see e1-REQ-4878)
	PolicyOrLegalNotice	O	If used, this element SHOULD contain a pointer to the epSOS framework agreement.
	HistoricalInformationPeriod	R	MUST be "0".
	PointersToOtherTSL	O	This element SHOULD NOT be used. NCPs MAY ignore any information that is provided in this element.
	ListIssueDateAndTime	R	MUST be used acc. to ETSI TS 102 231.
	NextUpdate	R	For epSOS pilot phase 1 this element MUST refer to the beginning of pilot phase 2 (acc to the TPM project plan). For epSOS pilot phase 2 this element MUST refer to the end of pilot phase 2.
	DistributionPoints	R	MUST point to the distribution point where the most current version of this epSOS NSL can be obtained.
	SchemeExtensions	O	MUST NOT be used for epSOS NSL.
TrustServiceProviderList		R	
	TrustServiceProvider	O	Information on NCP-A gateways and services
	TrustServiceProvider	O	Information on NCP-B gateways and services

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Signature	R	Confirmation on the authenticity of the epSOS NCP-Service Status List (see epSOS D3.7.2 for details).
-----------	---	---

Every NCP-Service Status List MUST be signed by its scheme operator. The XML signature MUST be applied by using the *tsl:TrustServiceStatusList/ds:Signature* element as defined below:

Signature Parameter	Usage Convention
CanonicalizationMethod	SHOULD be "http://www.w3.org/2001/10/xml-exc-c14n#"
Transformation	Exclusive XML canonicalization SHOULD be used (http://www.w3.org/2001/10/xml-exc-c14n# , acc. [W3C XMLDSig] and [W3C XML-EXC 1.0]). As inclusive namespaces other prefixes than the ones defined in e1-REQ-4874 MUST NOT be used.
SignatureMethod	The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see e1-REQ-4877). For signing epSOS NSL the signature method "http://www.w3.org/2000/09/xmldsig#rsa-sha1" SHOULD be used.
DigestMethod	The hash algorithm MUST comply with the epSOS recommendations on algorithms and key lengths (see e1-REQ-4877). For signing epSOS NSL the digest method "http://www.w3.org/2000/09/xmldsig#sha1" SHOULD be used.
KeyInfo	This element MUST contain a ds:X509Data element which contains the X.509 certificate of the NSL scheme operator.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.3.1.2.2 e1-REQ-1894 NCP Provider Identification

Within the <tsl:TrustServiceProviderList> element, an epSOS NSL MUST contain a single <tsl:TrustServiceProvider> element for each face of the NCP (NCP-A and/or NCP-B) that is operated by the respective member state. These elements MUST be used acc. to ETSI TS 102 231. A <tsl:TSPTradeName> element MUST be provided. It must be set to "NCP-A" for the provider of the inbound gateway and services and to "NCP-B" for the outbound gateway and service stubs.

The <tsl:TSPServices> list for each face of the NCP contains entries for the epSOS gateways and services of this NCP. The following table shows, which service entries are mandatory (M) or optional (O) for service providers (NCP-A) and service consumers (NCP-B).

Gateway / Service	Opt. NCP-A	Opt. NCP-B	Reference
epSOS VPN Gateway	R	R	
epSOS NCP	R	R	
epSOS Patient Identification Service	R	X	
epSOS Patient Service	O	X	
epSOS Order Service	O	X	
epSOS Dispensation Service	O	X	
epSOS Consent Service	O	X	
HCP Identity Provider	X	O	
HCP Signature CA	O	O	

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.2.3 e1-REQ-1895 epSOS VPN Gateway Status Information

epSOS VPN Gateways status information entries are used to announce the address and digital certificate of a NCP's VPN gateway.

TSL Element	Opt	Usage Convention	
TSPService	R		
ServiceInformation	R		
ServiceTypeIdentifier	R	MUST be “http://uri.epsos.eu/Svc/Svctype/VPNGateway”	
ServiceName	R	MUST be used acc. to ETSI TS 102 231.	
ServiceDigitalIdentity	R	Digital certificate(s) of the VPN gateway service	
DigitalId / X509Certificate	R	VPN gateway certificate (base64 encoded). Multiple gateway certificates MAY be provided. Each of these MUST comply with the epSOS VPN gateway certificate profile as defined in e1-REQ-1916 and e1-REQ-1917.	
Service Status	R	MUST be used acc. to ETSI TS 102 231. After epSOS pilot phase 1 NCPs MUST NOT connect to VPN gateways with a status other than “in accordance”.	
StatusStartTime	R	MUST be used acc. to ETSI TS 102 231.	
SchemeServiceDefinitionURI	X	MUST NOT be used for epSOS.	
ServiceSupplyPoints	R/-	Fully qualified domain names and/or IP-addresses of the VPN gateway. This field is required for NCP-A and MUST NOT be used for NCP-B. If multiple gateway addresses are given, NCP-B MAY select among these.	
TSPServiceDefinitionURI	X	MUST NOT be used for epSOS.	
ServiceInformationExtension	X	MUST NOT be used for epSOS.	
ServiceHistory	X	MUST NOT be used for epSOS.	

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Other fields than the ones listed above MUST NOT be provided for epSOS VPN Gateway status information. Other fields than the ones listed above MUST NOT be provided for epSOS VPN Gateway status information.

2.3.1.2.4 e1-REQ-1896 epSOS NCP Status Information

epSOS NCP status information list all certificates that are assigned to an NCP. NCP service providers and consumers MUST make use of only these certificates for authentication (TLS mutual trust establishment) and message signatures.

TSL Element	Opt	Usage Convention
TSPService	R	
ServiceInformation	R	
ServiceTypeIdentifier	R	MUST be "http://uri.epsos.eu/Svc/Svctype/NCP"
ServiceName	R	MUST be used acc. to ETSI TS 102 231.
ServiceDigitalIdentity	R	Digital certificates of the NCP
DigitalId / X509Certificate	R	NCP TLS certificate (base64 encoded). Multiple TLS certificates MAY be provided. For NCP-A each of these MUST comply with the epSOS TLS server certificate profile as defined e1-REQ-1919. For NCP-B each of these MUST comply with the epSOS TLS client certificate profile as defined in e1-REQ-1918.
DigitalId / X509Certificate	R	NCP signature certificate (base64 encoded). Multiple signature certificates MAY be provided. Each of these MUST comply with the epSOS NCP signature certificate profile as defined in e1-REQ-1920.
Service Status	R	MUST be used acc. to ETSI TS 102 231. After epSOS pilot phase 1 NCPs MUST NOT connect to other NCPs with a status other than "in accordance".
StatusStartingTime	R	MUST be used acc. to ETSI TS 102 231.
SchemeServiceDefinitionURI	X	MUST NOT be used for epSOS.
ServiceSupplyPoints	X	MUST NOT be used for epSOS.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

	TSPServiceDefinitionURI	X	MUST NOT be used for epSOS.
	ServiceInformationExtension	X	MUST NOT be used for epSOS.
	ServiceHistory	X	MUST NOT be used for epSOS.

Other fields than the ones listed above MUST NOT be provided for epSOS NCP status information.

2.3.1.2.5 e1-REQ-1897 epSOS Service Status Information

Service status information is used for announcing the web service endpoint addresses of the epSOS services.

TSL Element	Op t	Usage Convention
TSPService	R	
ServiceInformation	R	
ServiceTypeIdentifier	R	<p>MUST be used as follows:</p> <p>PatientIdentificationService service provider: “http://uri.epsos.eu/Svc/Svctype/PatientIdentificationService”</p> <p>epSOS PatientService service provider: “http://uri.epsos.eu/Svc/Svctype/PatientService”</p> <p>epSOS OrderService service provider: “http://uri.epsos.eu/Svc/Svctype/OrderService”</p> <p>epSOS DispensationService service provider: “http://uri.epsos.eu/Svc/Svctype/DispensationService”</p> <p>epSOS ConsentService service provider: “http://uri.epsos.eu/Svc/Svctype/ConsentService”</p>
ServiceName	R	MUST be used acc. to ETSI TS 102 231.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

	ServiceDigitalIdentity	R	MUST be empty.
	Service Status	R	MUST be used acc. to ETSI TS 102 231. After epSOS pilot phase 1 service consumers MUST NOT connect to service providers with a status other than "in accordance".
	StatusStartingTime	R	MUST be used acc. to ETSI TS 102 231.
	SchemeServiceDefinitionURI	X	MUST NOT be used for epSOS.
	ServiceSupplyPoints	R/-	Web service endpoint address of the service provider. If multiple WSE addresses are given, a service consumer MAY select among these.
	TSPServiceDefinitionURI	X	MUST NOT be used for epSOS.
	ServiceInformationExtension	X	MUST NOT be used for epSOS.
	ServiceHistory	X	MUST NOT be used for epSOS.

Other fields than the ones listed above MUST NOT be provided for epSOS service status information.

2.3.1.2.6 e1-REQ-1898 Use of Dedicated epSOS Identity Providers

epSOS country-B implementations MAY use dedicated Identity Providers within NCP-B for issuing HCP Identity Assertions. In this scenario the HCP Identity Assertion MUST be signed by the Identity Provider. Identity Provider status information can be used for distributing the Identity Provider certificate.

TSL Element	Opt	Usage Convention
TSPService	R	
ServiceInformation	R	
ServiceTypeIdentifier	R	MUST be "http://uri.etsi.org/Svc/Svctype/IdP"
ServiceName	R	MUST be used acc. to ETSI TS 102 231.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

	ServiceDigitalIdentity	R	Digital signature certificate of the Identity Provider
	DigitalId / X509Certificate	R	IdP signature certificate (base64 encoded). Multiple signature certificates MAY be provided. Each of these MUST comply with the epSOS NCP signature certificate profile as defined in e1-REQ-1920.
	Service Status	R	MUST be used acc. to ETSI TS 102 231. After epSOS pilot phase 1 NCPs MUST NOT accept assertions that were issued by a service with a status other than "in accordance".
	StatusStartingTime	R	MUST be used acc. to ETSI TS 102 231.
	SchemeServiceDefinitionURI	X	MUST NOT be used for epSOS.
	ServiceSupplyPoints	X	MUST NOT be used for epSOS.
	TSPServiceDefinitionURI	X	MUST NOT be used for epSOS.
	ServiceInformationExtension	X	MUST NOT be used for epSOS.
	ServiceHistory	X	MUST NOT be used for epSOS.

Other fields than the ones listed above MUST NOT be provided for epSOS IdP status information.

2.3.1.2.7 e1-TXT-751 Example epSOS NCP-Service Status List (NSL)

```
<?xml version="1.0" encoding="UTF-8"?>
<tsl:TrustServiceStatusList xmlns:tsl="http://uri.etsi.org/02231/v2#"
  Id="TrustServiceStatusList-1"
  TSLTag="http://uri.etsi.org/02231/TSLTag" >
  <tsl:SchemeInformation>
    <tsl:TSLVersionIdentifier>3</tsl:TSLVersionIdentifier>
    <tsl:TSLSequenceNumber>1</tsl:TSLSequenceNumber>
    <tsl:TSLType>http://uri.etsi.org/TrstSvc/TSLType/generic</tsl:TSLType>
    <tsl:SchemeOperatorName>
      <tsl:Name xml:lang="xx">Ministry of Health</tsl:Name>
    </tsl:SchemeOperatorName>
    <tsl:SchemeOperatorAddress>
      <tsl:PostalAddresses>
        <tsl:PostalAddress xml:lang="xx">
```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<tsl:StreetAddress>...</tsl:StreetAddress>
<tsl:Locality>...</tsl:Locality>
<tsl:PostalCode>...</tsl:PostalCode>
<tsl:CountryName>XX</tsl:CountryName>
</tsl:PostalAddress>
</tsl:PostalCodes>
<tsl:ElectronicAddress>
  <tsl:URI>mailto:epsos@health.gov.xx</tsl:URI>
  <tsl:URI>http://www.health.gov.xx/</tsl:URI>
</tsl:ElectronicAddress>
</tsl:SchemeOperatorAddress>
<tsl:SchemeName>
  <tsl:Name xml:lang="XX">XX:NCP-Service Status List: X-Country (XX)</tsl:Name>
</tsl:SchemeName>
<tsl:SchemeInformationURI>
  <tsl:URI xml:lang="xx">http://www.epsos.eu/docs/SecPol.pdf</tsl:URI>
  <tsl:URI xml:lang="xx">http://www.epsos.eu/docs/fwa.pdf</tsl:URI>
</tsl:SchemeInformationURI>
<tsl>StatusDeterminationApproach>
  http://uri.etsi.org/TrstSvc/StatusDetn/active
</tsl>StatusDeterminationApproach>
<tsl:SchemeTypeCommunityRules>
  <tsl:URI>http://www.epsos.eu</tsl:URI>
</tsl:SchemeTypeCommunityRules>
<tsl:SchemeTerritory>XX</tsl:SchemeTerritory>
<tsl:PolicyOrLegalNotice>
  <tsl:TSLPolicy>
    <tsl:URI xml:lang="xx">http://www.epsos.eu/docs/fwa.pdf</tsl:URI>
  </tsl:TSLPolicy>
</tsl:PolicyOrLegalNotice>
<tsl:HistoricalInformationPeriod>0</tsl:HistoricalInformationPeriod>
<tsl>ListIssueDateTime>2010-03-21T23:00:00Z</tsl>ListIssueDateTime>
<tsl:NextUpdate>
  <tsl:dateTime>2010-09-21T22:00:00Z</tsl:dateTime>
</tsl:NextUpdate>
<tsl:DistributionPoints>
  <tsl:URI>http://www.epsos.eu/tsl/xx/currenttsl.xml</tsl:URI>
</tsl:DistributionPoints>
</tsl:SchemeInformation>
<tsl:TrustServiceProviderList>
  <tsl:TrustServiceProvider>
    <tsl:TSPInformation>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

```

<tsl:TSPName>
  <tsl:Name xml:lang="xx">NCP Provider for XX</tsl:Name>
</tsl:TSPName>
<tsl:TSPTradeName>NCP-A</tsl:TSPTradeName>
<tsl:TSPAddress>
  <tsl:PostalAddresses>
    <tsl:PostalAddress xml:lang="xx">
      <tsl:StreetAddress>...</tsl:StreetAddress>
      <tsl:Locality>...</tsl:Locality>
      <tsl:PostalCode>1000</tsl:PostalCode>
      <tsl:CountryName>XX</tsl:CountryName>
    </tsl:PostalAddress>
  </tsl:PostalAddresses>
  <tsl:ElectronicAddress>
    <tsl:URI>mailto:office@ncp.epsos.xx</tsl:URI>
    <tsl:URI>http://www.ncp.epsos.xx/</tsl:URI>
  </tsl:ElectronicAddress>
</tsl:TSPAddress>
<tsl:TSPIInformationURI>
  <tsl:URI xml:lang="xx"> http://www.ncp.epsos.xx/docs/</tsl:URI>
</tsl:TSPIInformationURI>
</tsl:TSPIInformation>
<tsl:TSPServices>
  <tsl:TSPService>
    <tsl:ServiceInformation>
      <tsl:ServiceTypeIdentifier>
        http://uri.epsos.eu/TrstSvc/Svctype/VPNGateway
      </tsl:ServiceTypeIdentifier>
      <tsl:ServiceName>
        <tsl:Name xml:lang="xx">NCP-A VPN Gateway</tsl:Name>
      </tsl:ServiceName>
      <tsl:ServiceDigitalIdentity>
        <tsl:DigitalId>
          <tsl:X509Certificate>....</tsl:X509Certificate>
        </tsl:DigitalId>
      </tsl:ServiceDigitalIdentity>
      <tsl:ServiceStatus>
        http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
      </tsl:ServiceStatus>
      <tsl:StatusStartingTime>2009-09-21T12:37:33Z
      </tsl:StatusStartingTime>
    <tsl:ServiceSupplyPoints>

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

```

<tsl:URI>urn:gw:ncp:epsos:xx</tsl:URI>
</tsl:ServiceSupplyPoints>
</tsl:ServiceInformation>
<tsl:ServiceHistory/>
</tsl:TSPService>
<tsl:TSPService>
<tsl:ServiceInformation>
<tsl:ServiceTypelIdentifier>
http://uri.epsos.eu/TrstSvc/Svctype/NCP
</tsl:ServiceTypelIdentifier>
<tsl:ServiceName>
<tsl:Name xml:lang="xx">NCP-A Service Gateway</tsl:Name>
</tsl:ServiceName>
<tsl:ServiceDigitalIdentity>
<tsl:DigitalId>
<tsl:X509Certificate>....</tsl:X509Certificate>
</tsl:DigitalId>
<tsl:DigitalId>
<tsl:X509Certificate>....</tsl:X509Certificate>
</tsl:DigitalId>
</tsl:ServiceDigitalIdentity>
<tsl:ServiceStatus>
http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
</tsl:ServiceStatus>
<tsl>StatusStartingTime>2009-09-21T12:37:33Z
</tsl>StatusStartingTime>
</tsl:ServiceInformation>
<tsl:ServiceHistory/>
</tsl:TSPService>
<tsl:TSPService>
<tsl:ServiceInformation>
<tsl:ServiceTypelIdentifier>
http://uri.epsos.eu/TrstSvc/Svctype/PatientIdentificationService
</tsl:ServiceTypelIdentifier>
<tsl:ServiceName>
<tsl:Name xml:lang="xx">Patient Identification Service</tsl:Name>
</tsl:ServiceName>
<tsl:ServiceDigitalIdentity>
<tsl:ServiceStatus>
http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
</tsl:ServiceStatus>
<tsl>StatusStartingTime>2009-09-21T12:37:33Z

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

</tsl>StatusStartingTime>
<tsl:ServiceSupplyPoints>
  <tsl:URI>http://ncp.epsos.xx/svc/patientidentsvc</tsl:URI>
</tsl:ServiceSupplyPoints>
</tsl:ServiceInformation>
<tsl:ServiceHistory/>
</tsl:TSPService>
<tsl:TSPService>
  <tsl:ServiceInformation>
    <tsl:ServiceTypeIdentifier>
      http://uri.epsos.eu/TrstSvc/Svctype/ConsentService
    </tsl:ServiceTypeIdentifier>
    <tsl:ServiceName>
      <tsl:Name xml:lang="xx">Consent Service</tsl:Name>
    </tsl:ServiceName>
    <tsl:ServiceDigitalIdentity/>
    <tsl:ServiceStatus>
      http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
    </tsl:ServiceStatus>
    <tsl>StatusStartingTime>2009-09-21T12:37:33Z
    </tsl>StatusStartingTime>
    <tsl:ServiceSupplyPoints>
      <tsl:URI>http://ncp.epsos.xx/svc/consentsvc</tsl:URI>
    </tsl:ServiceSupplyPoints>
  </tsl:ServiceInformation>
  <tsl:ServiceHistory/>
</tsl:TSPService>
<tsl:TSPService>
  <tsl:ServiceInformation>
    <tsl:ServiceTypeIdentifier>
      http://uri.epsos.eu/TrstSvc/Svctype/PatientService
    </tsl:ServiceTypeIdentifier>
    <tsl:ServiceName>
      <tsl:Name xml:lang="xx">Patient Service</tsl:Name>
    </tsl:ServiceName>
    <tsl:ServiceDigitalIdentity/>
    <tsl:ServiceStatus>
      http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
    </tsl:ServiceStatus>
    <tsl>StatusStartingTime>2009-09-21T12:37:33Z
    </tsl>StatusStartingTime>
    <tsl:ServiceSupplyPoints>
  
```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<tsl:URI>http://ncp.epsos.xx/svc/patientsvc</tsl:URI>
</tsl:ServiceSupplyPoints>
</tsl:ServiceInformation>
<tsl:ServiceHistory/>
</tsl:TSPService>
</tsl:TSPServices>
</tsl:TrustServiceProvider>
<tsl:TrustServiceProvider>
<tsl:TSPIInformation>
  <tsl:TSPName>
    <tsl:Name xml:lang="xx">NCP Provider for XX</tsl:Name>
  </tsl:TSPName>
  <tsl:TSPTradeName>NCP-B</tsl:TSPTradeName>
  <tsl:TSPAddress>
    <tsl:PostalAddresses>
      <tsl:PostalAddress xml:lang="xx">
        <tsl:StreetAddress>...</tsl:StreetAddress>
        <tsl:Locality>...</tsl:Locality>
        <tsl:PostalCode>1000</tsl:PostalCode>
        <tsl:CountryName>XX</tsl:CountryName>
      </tsl:PostalAddress>
    </tsl:PostalAddresses>
    <tsl:ElectronicAddress>
      <tsl:URI>mailto:office@ncp.epsos.xx</tsl:URI>
      <tsl:URI>http://www.ncp.epsos.xx/</tsl:URI>
    </tsl:ElectronicAddress>
  </tsl:TSPAddress>
  <tsl:TSPIInformationURI>
    <tsl:URI xml:lang="xx"> http://www.ncp.epsos.xx/docs/</tsl:URI>
  </tsl:TSPIInformationURI>
</tsl:TSPIInformation>
<tsl:TSPServices>
  <tsl:TSPService>
    <tsl:ServiceInformation>
      <tsl:ServiceTypelIdentifier>
        http://uri.epsos.eu/TrstSvc/Svctype/VPNGateway
      </tsl:ServiceTypelIdentifier>
      <tsl:ServiceName>
        <tsl:Name xml:lang="xx">NCP-B VPN Gateway</tsl:Name>
      </tsl:ServiceName>
      <tsl:ServiceDigitalIdentity>
        <tsl:DigitalId>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<tsl:X509Certificate>....</tsl:X509Certificate>
</tsl:DigitalId>
</tsl:ServiceDigitalIdentity>
<tsl:ServiceStatus>
  http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
</tsl:ServiceStatus>
<tsl:StatusStartingTime>2009-09-21T12:37:33Z
</tsl:StatusStartingTime>
<tsl:ServiceSupplyPoints>
  <tsl:URI>urn:gw:ncp:epsos:xx</tsl:URI>
</tsl:ServiceSupplyPoints>
</tsl:ServiceInformation>
<tsl:ServiceHistory/>
</tsl:TSPService>
<tsl:TSPService>
  <tsl:ServiceInformation>
    <tsl:ServiceTypeIdentifier>
      http://uri.epsos.eu/TrstSvc/Svctype/NCP
    </tsl:ServiceTypeIdentifier>
    <tsl:ServiceName>
      <tsl:Name xml:lang="xx">NCP-B Service Gateway</tsl:Name>
    </tsl:ServiceName>
    <tsl:ServiceDigitalIdentity>
      <tsl:DigitalId>
        <tsl:X509Certificate>....</tsl:X509Certificate>
      </tsl:DigitalId>
      <tsl:DigitalId>
        <tsl:X509Certificate>....</tsl:X509Certificate>
      </tsl:DigitalId>
    </tsl:ServiceDigitalIdentity>
    <tsl:ServiceStatus>
      http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
    </tsl:ServiceStatus>
    <tsl:StatusStartingTime>2009-09-21T12:37:33Z
    </tsl:StatusStartingTime>
    </tsl:ServiceInformation>
    <tsl:ServiceHistory/>
  </tsl:TSPService>
  </tsl:TSPServices>
</tsl:TrustServiceProvider>
</tsl:TrustServiceProviderList>
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Id="....">

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

....
</dsig:Signature>
</tsl:TrustServiceStatusList>

2.3.1.3 e1-REQ-1835 epSOS Audit Trail Common Specification

Related to e1-REQ-4636 NCP Audit Trial Interface and Functionality

Related to e1-REQ-4591 REQ 3.3.6 Secure Context Establishment

All epSOS service consumers and service providers MUST write audit trails for all message exchange operations as well as for exceptions encountered.

2.3.1.3.1 e1-TXT-741 Note

The main objective of the audit trail written at the country of the patient's affiliation is to protect the patient's privacy. The main objective of the audit trail written at the country of care is to protect the acting health professional's reputation and to protect him from false accusations. epSOS only defines the schema for exporting audit trails and by this makes sure that audit data can be assessed for post-mortem security and privacy issues in a uniform manner. The transport of audit trail data to the audit repository is national concern and only governed by the epSOS security concept. Exchange of audit data among countries is a sole organisational issue and not covered by this specification.

2.3.1.3.2 e1-REQ-1836 Referenced Standards

The epSOS Audit Trail specification builds upon the following set of standards and profiles:

RFC3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications RFC 3881

Regarding the concrete use of RFC 3881 epSOS borrows coded values and extension mechanisms from:

DICOM Supplement 95: Audit Trail Messages.DICOM Sup95

IHE ATNA: IHE IT Infrastructure Technical Framework – Audit Trail and Node Authentication Profile IHE ITI TF-2a August 2009

Following the conventions of IHE, coded values within audit trail entries are restricted to the attributes "@code", "@codeSystemName" and "@displayName" and denoted as EV (code, codeSystemName, displayName).

2.3.1.3.2.1 e1-TXT-742 Note

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The original audit trail encodings of the IHE transactions that lay ground for epSOS services are always used as a starting point for the epSOS audit trail entry definitions. Nevertheless a full compatibility could not be reached due to the extended requirements of epSOS on privacy and non-repudiation D3.7.2

2.3.1.3.3 e1-REQ-1837 RFC 3881 Overview and epSOS Audit Schemas

For epSOS three different Audit Trail schemas are derived from the RFC 3881 categories. Table 3 lists the defined epSOS audit schemas.

Schema	Used By	Description
HCP Assurance	Service Consumer (country B)	The HCP Assurance audit schema is used by the service consumer at the country of care. The main purpose of this audit trail is to track all actions of this country's HPs in order to protect them against false accusations for not properly using the possibilities of epSOS (e. g. a patient claiming that a HP did not access his data even though he authorised him to do so).
Patient Privacy	Service Provider (country A)	The Patient Privacy audit schema is used by the service provider at the patient's country of affiliation. The main purpose of this audit trail is to empower the patient to get knowledge on all usages of his medical data. By analysing this audit trail the patient is able to evaluate the legitimacy of all accesses to his data.
Patient ID Mapping	Service Provider (country A)	During patient identification the identifier provided by the patient is mapped onto a patient identifier that is to be used for subsequent calls. The patient ID mapping audit schema MAY be written to a log file that is separated from the Patient Privacy Audit Log in cases where a member state makes use of pseudonyms (by separating the logs the Patient Privacy Audit trail is pseudonymous while the Patient ID Audit trail can be used for resolving pseudonyms for further privacy assessments).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

--	--	--

Each schema is used for a separate audit trail. The Patient ID Mapping trail SHOULD be written and stored by a separated system. A linkage of these trails MUST comply with the respective national legislation of the country where the audit trail is written. A linkage of audit trails that are written by different NCPs in different countries MUST comply with the respective epSOS security regulations, communities, and service level agreements. The payload of each auditable event SHOULD be safeguarded by a payload signature that is protecting the auditable event written as of RFC 3881 as a whole.

2.3.1.3.3.1 e1-TXT-743 Note

RFC 3881 defines five categories that are subject to audit activity:

Event Identification – What was done?

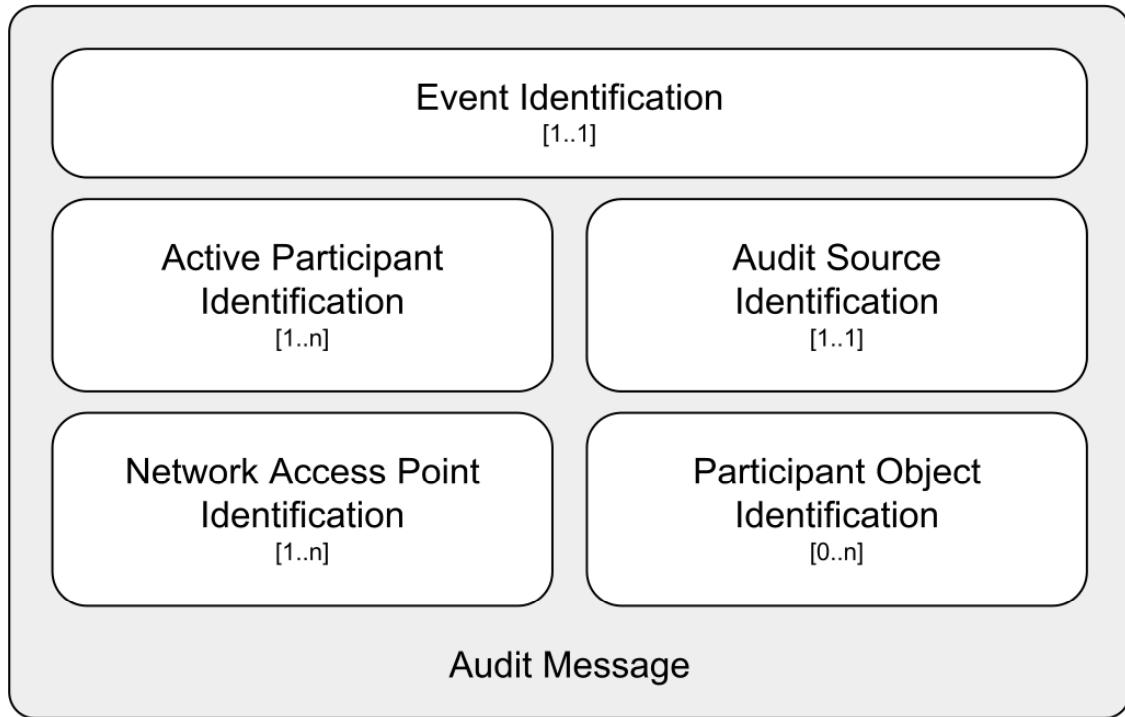
Active Participant Identification – By whom?

Network Access Point Identification – Initiated from where?

Audit Source Identification – Using which server?

Participant Object Identification – For which patient? To what record?

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



2.3.1.3.4 e1-REQ-1838 epSOS HCP Assurance Audit Schema

Related to e1-REQ-4923 Discard() Operation Security and Audit Considerations

Related to e1-REQ-4942 Discard() Operation Security and Audit Considerations

Related to e1-REQ-4904 epSOS Order Service Security Audit Considerations

Related to e1-REQ-4887 epSOS Patient Service Security Audit Considerations

Related to e1-REQ-4925 Initialize() Operation Security and Audit Considerations

Related to e1-REQ-4941 Put() Operation Security and Audit Considerations

The HCP Assurance Audit schema consists of the following subcategories of the original categories as defined by RFC 3881.

RFC 3881 Category	epSOS Instance	Description
Event	Event	Audited event according to RFC 3881
Active Participant	Requesting Point of	Point of Care that is the origin of the event

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

	Care	
	Human Requestor	HP who triggered the event
	Service Consumer NCP	Service consumer NCP that triggered the event
	Service Provider NCP	Destination of the event
Audit Source	Audit Source	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Participant Object	Patient	Patient whose data is affected from the event
	Event Target	Target of the event
	Error Message	Optional: Information on errors that occurred during transaction processing

Entries according to this schema MUST only be written after receipt of the response to the transaction that is target to auditing.

In the following requirements the required (R) and optional (O) fields of these categories are listed. Fields not listed here but defined in RFC 3881 MAY be defined by the operator of the service consumer nodes or by the NCP of the country of care. In cases where audit trail entries are exchanged between NCPs, these fields SHOULD be blanked.

2.3.1.3.4.1 e1-REQ-1844 Event Identification

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(<i>num</i> , "epSOS Transaction", <i>name</i>) where <i>num</i> is the number of the transaction including the "epSOS-" prefix and <i>name</i> is the name of the transaction as written in the respective Use Case Roles diagram. See e1-REQ-1876 for a full list of all EventIDs defined for epSOS.
EventActionCode	R	Acc. RFC 3881. See e1-REQ-1876 for a mapping of EventIDs and EventActionCodes.
EventDateTime	R	Acc. RFC 3881. Time MUST be provided by a node that is grouped with a Consistent Time Consumer

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

		Actor.
EventOutcomeIndicator	R	Acc. RFC 3881. MUST be "0" on full success, "1" in case of a partial delivery, "4" for temporal or recoverable failures, and "8" for permanent failures.

2.3.1.3.4.2 e1-REQ-1845 Active Participant Identification: Point of Care

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the point of care that initiated the event. This field MUST contain the name of the point of care as provided by the HCP Identity Assertion (see e1-REQ-1901).
UserIsRequestor	R	"true"
RoleIDCode	R	RFC 3881 compliant encoding of the kind of HPO as defined in the "HCPO Type" attribute of the Authentication Assertion that was issued for the user.

2.3.1.3.4.3 e1-REQ-1846 Active Participant Identification: Human Requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HP who initiated the event. This field MUST contain the name identifier as given in the respective element of the Authentication Assertion that was issued for this user. See e1-REQ-1878 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HP as given in the Subject-ID attribute of the HCP identity assertion (see e1-REQ-1906).
AlternativeUserID	O	UUID of the original Authentication Assertion that was issued for this user. This field SHOULD only be used if the issued epSOS Authentication Assertion is an attest for an Assertion that was issued by the national infrastructure. In this scenario the UUID might be useful to univocally link these two assertions.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

UserIsRequestor	R	“true”
RoleIDCode	R	RFC 3881 compliant encoding of the user’s role as defined in the “role” attribute of the Identity Assertion that was issued for this user.

2.3.1.3.4.4 e1-REQ-1847 Active Participant Identification: Service Consumer NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that triggered the epSOS operation that corresponds to the event
UserIsRequestor	R	“true”
RoleIDCode	R	Coded value for “epSOS Service Consumer”

2.3.1.3.4.5 e1-REQ-1848 Active Participant Identification: Service Provider NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that processed the epSOS operation that corresponds to the event
UserIsRequestor	R	“false”
RoleIDCode	R	Coded value for “epSOS Service Provider”

2.3.1.3.4.6 e1-REQ-1849 Audit Source

Field Name	Opt.	Value Constraints
AuditSourceID	R	Identifies the authority that is legally responsible for the audit source. In the case of epSOS this element MUST provide the ISO 3166-2 code of the country/region where the audit source is located.

 <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.4.7 e1-REQ-1850 Participant Object: Patient

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "1" (Person)
ParticipantObjectTypeCodeRole	R	MUST be "1" (Patient)
ParticipantObjectIDTypeCode	R	EV(2, RFC-3881, "Patient Number")
ParticipantObjectID	R	Patient identifier encoded in HL7 II format. Only the patient identifier that is issued during the patient identification handshake MUST be used for this field.

 epSOS <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.4.8 e1-REQ-1851 Participant Object: Error Message

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "3" (Report)
ParticipantObjectIDTypeCode	R	MUST be "9" (Report Number)
ParticipantObjectID	R	String-encoded error code that was included with the response message.
ParticipantObjectDetail	R	Error message as included with the response message as a type-value pair acc to [RFC 3881]. As a type qualifier "errormsg" MUST be used. The value MUST contain the base64 encoded error message.

A single error message section MUST be given for each error code/message that is included with a response message.

2.3.1.3.4.9 e1-REQ-1852 Participant Object: Event Target

This subcategory MUST be defined individually for each transaction.

2.3.1.3.5 e1-REQ-1839 epSOS Patient Privacy Audit Schema

Related to e1-REQ-4923 Discard() Operation Security and Audit Considerations

Related to e1-REQ-4942 Discard() Operation Security and Audit Considerations

Related to e1-REQ-4904 epSOS Order Service Security Audit Considerations

Related to e1-REQ-4887 epSOS Patient Service Security Audit Considerations

Related to e1-REQ-4925 Initialize() Operation Security and Audit Considerations

Related to e1-REQ-4941 Put() Operation Security and Audit Considerations

The Patient Privacy Audit schema consists of the following subcategories of the original categories as defined by RFC 3881.

 <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

RFC 3881 Category	epSOS Instance	Description
Event	Event	Audited event according to RFC 3881
Active Participant	Human Requestor	HP who triggered the event
	Service Consumer NCP	Service consumer NCP that triggered the event
	Service Provider NCP	Destination of the event
Audit Source	Audit Source	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Participant Object	Patient	Patient whose data is affected from the event
	Event Target	Target of the event
	Error Message	Optional: Information on errors that occurred during transaction processing

Entries according to this schema MUST only be written after the response to the transaction that is target to auditing has been successfully transmitted to the requesting gateway.

In the following requirements the required (R) and optional (O) fields of these categories are listed. Fields not listed here but defined in RFC 3881 MAY be defined by the operator of the Inbound Gateway or by the NCP of the country of affiliation. In cases where audit trail entries are exchanged between NCPs, these fields SHOULD be blanked.

 epSOS <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.5.1 e1-REQ-1853 Event Identification

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(<i>num</i> , “epSOS Transaction”, <i>name</i>) where <i>num</i> is the number of the transaction including the “epSOS-“ prefix and <i>name</i> is the name of the transaction as written in the respective Use Case Roles diagram. See e1-REQ-1876 for a full list of all eventIDs defined for epSOS.
EventActionCode	R	Acc. RFC 3881. See e1-REQ-1876 for a mapping of EventIDs and EventActionCodes.
EventDateTime	R	Acc. RFC 3881. Time MUST be provided by a node that is grouped with a Consistent Time Consumer Actor.
EventOutcomeIndicator	R	Acc. RFC 3881. MUST be “0” on full success, “1” in case of a partial delivery, “4” for temporal or recoverable failures, and “8” for permanent failures.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.5.2 e1-REQ-1854 Active Participant Identification: Human Requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HP who initiated the event. This field MUST contain the name identifier as given in the respective element of the Authentication Assertion that was issued for this user. See e1-REQ-1878 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HP as given in the Subject-ID attribute of the HCP identity assertion (see e1-REQ-1906).
UserIsRequestor	R	“true”
RoleIDCode	R	RFC 3881 compliant encoding of the user’s role as defined in the “role” attribute of the Identity Assertion that was issued for this user.

2.3.1.3.5.3 e1-REQ-1855 Active Participant Identification: Service Consumer NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that triggered the epSOS operation that corresponds to the event
UserIsRequestor	R	“true”
RoleIDCode	R	Coded value for “epSOS Service Consumer”

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.5.4 e1-REQ-1856 Active Participant Identification: Service Provider NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that processed the epSOS operation that corresponds to the event
UserIsRequestor	R	“false”
RoleIDCode	R	Coded value for “epSOS Service Provider”

2.3.1.3.5.5 e1-REQ-1857 Audit Source

Field Name	Opt.	Value Constraints
AuditSourceID	R	Identifies the authority that is legally responsible for the audit source. In the case of epSOS this element MUST provide the ISO 3166-2 code of the country/region where the audit source is located.

2.3.1.3.5.6 e1-REQ-1858 Participant Object: Patient

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “1” (Person)
ParticipantObjectTypeCodeRole	R	MUST be “1” (Patient)
ParticipantObjectIDTypeCode	R	EV(2, RFC-3881, “Patient Number”)
ParticipantObjectID	R	Patient identifier encoded in HL7 II format. Only the patient identifier that is issued during the patient identification handshake MUST be used for this field.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.5.7 e1-REQ-1859 Participant Object: Error Message

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "3" (Report)
ParticipantObjectIDTypeCode	R	MUST be "9" (Report Number)
ParticipantObjectID	R	String-encoded error code that was included with the response message.
ParticipantObjectDetail	R	Error message as included with the response message as a type-value pair acc to RFC 3881. As a type qualifier "errormsg" MUST be used. The value MUST contain the base64 encoded error message.

A single error message section MUST be given for each error code/message that is included with a response message.

2.3.1.3.5.8 e1-REQ-1860 Participant Object: Event Target

This subcategory MUST be defined individually for each transaction.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.6 e1-REQ-1840 epSOS Patient ID Mapping Audit Schema

Related to e1-REQ-4871 epSOS Identification Service Security Audit Considerations

The Patient ID Mapping Audit schema consists of the following subcategories of the original categories as defined by RFC 3881.

RFC 3881 Category	epSOS Instance	Description
Event	Event	Audited event according to RFC 3881
Active Participant	Human Requestor	HP who triggered the event
	Service Consumer NCP	Service consumer NCP that triggered the event
	Service Provider NCP	Destination of the event
	Mapping Service	Service that provided the mapping
Audit Source	Audit Source	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Participant Object	Patient Source	Patient whose identifier was mapped
	Patient Target	Result of the mapping operation
	Error Message	Optional: Information on errors that occurred during transaction processing

Entries according to this schema MUST only be written after the response to the mapping transaction that is target to auditing has been successfully transmitted to the requesting gateway.

In the following requirements the required (R) and optional (O) fields of these categories are listed. Fields not listed here but defined in RFC 3881 MAY be defined by the operator of the Inbound Gateway or by the NCP of the country of affiliation. In cases where audit trail entries are exchanged between NCPs, these fields SHOULD be blanked.

2.3.1.3.6.1 e1-REQ-1861 Event Identification

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(<i>num</i> , “epSOS Transaction”, <i>name</i>) where <i>num</i> is the number of the transaction including the “epSOS-“ prefix and <i>name</i> is the name of the transaction as written in the respective Use Case Roles diagram. See e1-REQ-1876 for a full list of all eventIDs defined for epSOS.
EventActionCode	R	Acc. RFC 3881. See e1-REQ-1876 for a mapping of EventIDs and EventActionCodes.
EventDateTime	R	Acc. RFC 3881. Time MUST be provided by a node that is grouped with a Consistent Time Consumer Actor.
EventOutcomeIndicator	R	Acc. RFC 3881. MUST be “0” on successful patient identification, “1” in case of multiple matches, “4” in case of insufficient traits data, and “8” for permanent failures.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

2.3.1.3.6.2 e1-REQ-1862 Active Participant Identification: Human Requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HP who initiated the event. This field MUST contain the name identifier as given in the respective element of the Authentication Assertion that was issued for this user. See e1-REQ-1878 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HP as given in the Subject-ID attribute of the HCP identity assertion (see e1-REQ-1906).
UserIsRequestor	R	“true”
RoleIDCode	R	RFC 3881 compliant encoding of the user’s role as defined in the “role” attribute of the Identity Assertion that was issued for this user.

2.3.1.3.6.3 e1-REQ-1863 Active Participant Identification: Service Consumer NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that triggered the epSOS operation that corresponds to the event
UserIsRequestor	R	“true”
RoleIDCode	R	Coded value for “epSOS Service Consumer”

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.6.4 e1-REQ-1864 Active Participant Identification: Service Provider NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that processed the epSOS operation that corresponds to the event
UserIsRequestor	R	“false”
RoleIDCode	R	Coded value for “epSOS Service Provider”

2.3.1.3.6.5 e1-REQ-1865 Active Participant Identification: Mapping Service

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded OID of the service instance that performed the mapping (e. g. a national MPI)
UserIsRequestor	R	“false”
RoleIDCode	R	Coded value for “Master Patient Index” or “Pseudonymisation”

2.3.1.3.6.6 e1-REQ-1866 Audit Source

Field Name	Opt.	Value Constraints
AuditSourceID	R	Identifies the authority that is legally responsible for the audit source. In the case of epSOS this element MUST provide the ISO 3166-2 code of the country/region where the audit source is located.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.6.7 e1-REQ-1867 Participant Object: Patient Source

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "1" (Person)
ParticipantObjectTypeCodeRole	R	MUST be "1" (Patient)
ParticipantObjectIDTypeCode	R	EV(2, RFC-3881, "Patient Number")
ParticipantObjectID	R	Patient identifier encoded in HL7 II format. Only the patient identifier that was the source for the mapping MUST be used for this field.

2.3.1.3.6.8 e1-REQ-1868 Participant Object: Patient Target

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "1" (Person)
ParticipantObjectTypeCodeRole	R	MUST be "1" (Patient)
ParticipantObjectIDTypeCode	R	EV(2, RFC-3881, "Patient Number")
ParticipantObjectID	R	Patient identifier encoded in HL7 II format. Only the patient identifier that was the result for the mapping MUST be used for this field.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

2.3.1.3.6.9 e1-REQ-1869 Participant Object: Error Message

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “2” (System Object)
ParticipantObjectTypeCodeRole	R	MUST be “3” (Report)
ParticipantObjectIDTypeCode	R	MUST be “9” (Report Number)
ParticipantObjectID	R	String-encoded error code that was included with the response message.
ParticipantObjectDetail	R	Error message as included with the response message as a type-value pair acc to RFC 3881. As a type qualifier “errormsg” MUST be used. The value MUST contain the base64 encoded error message.

A single error message section MUST be given for each error code/message that is included with a response message.

2.3.1.3.7 e1-REQ-1841 Audit Trail Data for Non-Repudiation

For traceability and non-repudiation of message exchange operations, D3.7.2 requires that the full security headers (including body signature and security token) of all messages MUST be written to audit trails at both NCP-A and NCP-B.

NCP implementors MUST consider the following requirements to the message audit trail entries of all epSOS audit schemas as specified in e1-REQ-1835.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.7.1 e1-REQ-1870 Participant Object: Request Message

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "4" (Other)
ParticipantObjectIDTypeCode	R	MUST be EV("req", "epSOS Msg", "Request Message")
ParticipantObjectID	R	String-encoded UUID of the request message
ParticipantObjectDetail	R	Full security header of the request message as a type-value pair acc to RFC 3881. As a type qualifier "securityheader" MUST be used. The value MUST contain the base64 encoded security header.

2.3.1.3.7.2 e1-REQ-1871 Participant Object: ResponseMessage

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "4" (Other)
ParticipantObjectIDTypeCode	R	MUST be EV("rsp", "epSOS Msg", "Response Message")
ParticipantObjectID	R	String-encoded UUID of the response message
ParticipantObjectDetail	R	Full security header of the response message as a type-value pair acc to RFC 3881. As a type qualifier "securityheader" MUST be used. The value MUST contain the base64 encoded security header.

As RFC5424 defines a recommended message size of 2048 bytes an NCP implementation MUST store the ParticipantObjectDetail attribute value data outside the audit trail and just place a reference to this data into the audit trail entry.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.3.1.3.8 e1-REQ-1842 Audit Trail Entries on Internal Activities

2.3.1.3.8.1 e1-REQ-1872 Issuance of a HCP Identity Assertion

The NCP of the country of care MUST write an audit trail entry for the confirmation of a HP authentication (e. g. after the attesting signature has been applied to the Identity Assertion). The audit message MUST be assembled according to the HCP Assurance audit schema as defined in e1-REQ-1838. The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event. See e1-REQ-1876 for the respective values.
Requesting Point of Care	R	Organisation that performed the initial identification and authentication of the HP (e. g. a hospital)
Human Requestor	R	HP whose authenticity was attested
Source Gateway	O	Service that performed the original authentication of the HP
Target Gateway	R	NCP-B that attested the authenticity of the Identity Assertion
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	X	
Event Target	R	See below

 epsOS <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

For the event target, a reference to the assertion MUST be kept in order to allow for a linkage of assertions used within messages to their issuing act.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectIDTypeCode	R	MUST be EV("IdA", "epsOS Security", "HCP Identity Assertion")
ParticipantObjectID	R	String-encoded UUID of the assertion

2.3.1.3.8.2 e1-REQ-1873 Issuance of a Treatment Relationship Confirmation Assertion

The NCP at the country of care MUST write an audit trail entry for the confirmation of a treatment relationship between a HP(O) and a patient. The audit message MUST be assembled according to the HCP Assurance audit schema as defined in e1-REQ-1838. The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epsOS Instance	Opt.	Description
Event	R	Audited event. See e1-REQ-1876 for the respective values.
Requesting Point of Care	R	Organisation that established a treatment relationship with the patient (e. g. a hospital)
Human Requestor	R	HP who acts on behalf of the HPO.
Source Gateway	O	System at the HPO that requested the issuance of the TRC assertion
Target Gateway	R	NCP-B that attested the existence of the treatment relationship
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	R	Patient who is treated by the HPO
Event Target	R	See below

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

For the event target, a reference to the assertion MUST be kept in order to allow for a linkage of assertions used within messages to their issuing act.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectIDTypeCode	R	MUST be EV("TrcA", "epSOS Security", "TRC Assertion")
ParticipantObjectID	R	String-encoded UUID of the assertion

2.3.1.3.8.3 e1-REQ-1874 Import of an epSOS NCP Trusted Service List

An NCP MUST write an audit trail entry for the import of another NCPs Trusted Service List. The audit message MUST be assembled according to the HCP Assurance audit schema as defined in e1-REQ-1838. The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event. See e1-REQ-1876 for the respective values.
Requesting Point of Care	X	
Human Requestor	X	
Source Gateway	R	URL of the NSL providing service
Target Gateway	R	NCP that imported the NSL
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	X	
Event Target	R	See below

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

For the event target, a reference to the NSL MUST be written.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectIDTypeCode	R	MUST be EV("NSL", "epSOS Security", "Trusted Service List")
ParticipantObjectID	R	@ID of the NSL + " " + string encoded SequenceNumber of the NSL

2.3.1.3.8.4 e1-REQ-1875 Pivot Translation of a Medical Document

An NCP MUST write an audit trail entry for the pivot translation of a medical document. The audit message MUST be assembled according to the HCP Assurance audit schema as defined in e1-REQ-1838. The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event. See e1-REQ-1876 for the respective values.
Requesting Point of Care	X	
Human Requestor	X	
Source Gateway	X	
Target Gateway	R	Identification of the NCP Translation Service
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	X	
Event Target	R	See below

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

An event target MUST be defined for both the source data of the translation and the result of the translation.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "4" (other)
ParticipantObjectDataLifeCycle	R	MUST be "5" (translation)
ParticipantObjectIDTypeCode	R	MUST be EV("in", "epSOS Tranlation", "Input Data")
ParticipantObjectID	R	Identifier that allows to univocally identify the source document or source data entries.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "4" (other)
ParticipantObjectDataLifeCycle	R	MUST be "5" (translation)
ParticipantObjectIDTypeCode	R	MUST be EV("out", "epSOS Tranlation", "Output Data")
ParticipantObjectID	R	Identifier that allows to univocally identify the target document.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.3.1.3.8.5 e1-REQ-4876 Documentation of the Patient Information Notification (PIN)

Related to e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

The NCP at the country of care MUST write an audit trail entry documenting the confirmation of the HP concerning the issuance and approval of the Patient Information Notification (PIN) between a HP(O) and a patient. The audit message MUST be assembled according to the HCP Assurance audit schema as defined in e1-REQ-1838. The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event. See e1-REQ-1876 for the respective values.
Requesting Point of Care	R	Organisation that established a treatment relationship with the patient (e. g. a hospital) and is responsible for collecting the PIN.
Human Requestor	R	HP who acts on behalf of the HPO.
Source Gateway	O	System at the HPO
Target Gateway	R	NCP-B that attested the existence of the treatment relationship
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	R	Patient who is treated by the HPO
Event Target	R	See below

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

For the event target, a reference to the assertion MUST be kept in order to allow for a linkage of assertions used within messages to their issuing act.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "4" (Other)
ParticipantObjectIDTypeCode	R	MUST be EV("PIN", "epSOS Security", "Privacy Information Notice")
ParticipantObjectDataLifecycle	R	MUST be "12" (Receipt of Disclosure)
ParticipantObjectID	R	string-encoded of either "PINack" for consent given OR "PINdny" for consent denied

2.3.1.3.9 e1-REQ-1843 epSOS-specific Codes and Encodings for RFC3881

In the following sections epSOS-specific code lists and encoding conventions for use within audit trail entries are defined.

2.3.1.3.9.1 e1-REQ-1876 epSOS EventIDs

Service	Operation	Event ID	Event Name	Action
epSOSIdentificationService	FindIdentityByTraits	epso s-11	eposIdentityService::FindIdentityByTraits	"E"
epSOSPatientService	List	epso s-21	eposPatientService::List	"R"
epSOSOrderService	List	epso s-31	eposOrderService::List	"R"
epSOSDispensationService	Initialize	epso s-41	eposDispensationService::Initialize	"U"
	Discard	epso s-42	eposDispensationService::Discard	"D"
epSOSConsentService	Put	epso s-51	eposConsentService::Put	"U"

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3	
	Version:	1.0
D5.2.3	Date:	31/01/2013

	Discard	epso s-52	epsosConsentService::Discard	"D"
	-	epso s-53	epSOSConsentService::PIN	"R"
Country-B Identity Provider	Issuance of HCP Identity Assertion	epso s-91	identityProvider::HcpAuthentication	"E"
Country-B NCP	Issuance of a TRC Assertion	epso s-92	ncp::TrcAssertion	"E"
Configuration Manager	NSL Import	epso s-93	ncpConfigurationManager::ImportN SL	"E"
Transformation Manager	Pivot Translation	epso s-94	ncpTransformationMgr::Translate	"E"

In error cases where NCP-A cannot decode the requested operation an event ID of EV(epsos-00, "unknown", unknown) MUST be written to the Patient Privacy Audit Trail.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.3.9.2 e1-REQ-1877 Active Participant Role ID Codes

Codesystem	Code	DisplayName
epSOS	ServiceProvider	epSOS Service Consumer
epSOS	ServiceConsumer	epSOS Service Provider
epSOS	Pseudonymisation	Pseudonymisation Service
epSOS	MasterPatientIndex	Master Patient Index
epSOS	IdentityProvider	NCP Identity Provider
epSOS	NCP-B	NCP-B
epSOS	Configuration Manager	NCP Configuration Manager
epSOS	Transformation Manager	NCP Transformation Manager

2.3.1.3.9.3 e1-REQ-1878 Encoding of the User Identifier

The HP identifier entry MUST be taken from the subject field of the identification assertion that is transmitted together with a request. For conformance with IHE XUA++ the following encoding MUST be used:

```
SPProvidedID<saml:SubjectNameID@saml:Issuer>
```

The SPProvidedID is needed because there are situations where identity federation is in place. The SPProvidedID is a name identifier established by a service provider or affiliation of providers for the entity in the NameID different from the primary name identifier given in the content of the element.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.3.1.4 e1-REQ-1899 epSOS Profiles on Assertions and Certificates

Related to e1-REQ-4591 REQ 3.3.6 Secure Context Establishment

epSOS security mechanisms MUST build upon SAML assertions and digital certificates as core security objects. The following requirements provide the respective epSOS security object profiles on SAML and X.509.

2.3.1.4.1 e1-REQ-1901 HCP Identity Assertion

Related to e1-REQ-1981 HP-B Identification and Authentication

Related to e1-REQ-4877 Cryptographic Keys and Algorithms

Being part of the epSOS security architecture, the national and therefore decentralized identity management produces authentication assertions that are encoded as SAML assertions according to OASIS SAML 2.0. Such an assertion confirms the user's identity, the successful authentication of the user, and the attributes assigned to the user.

The HCP Identity Assertion is a profiled SAML v2.0 assertion. It has *Sender-Vouches* configured as the confirmation method.

2.3.1.4.2 e1-TXT-744 Note

The *HCP Identity Assertion* defines a means to communicate a user's assigned identity and its attributes in a trustworthy manner among NCPs. This enables relying parties to run their business tasks without identifying the requester since this is done by a trusted third-party authentication service. On behalf of the "transferrable" claim the relying party is able to render and enforce access decisions.

2.3.1.4.3 e1-REQ-1904 Generic Structure of the Identity Assertion

The following figure gives an overview of the top level elements of the SAML assertion type. The Assertion element is of the AssertionType complex type. The following summary gives an overview of how sub elements are used with regard to the context of the epSOS Identity Assertion.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

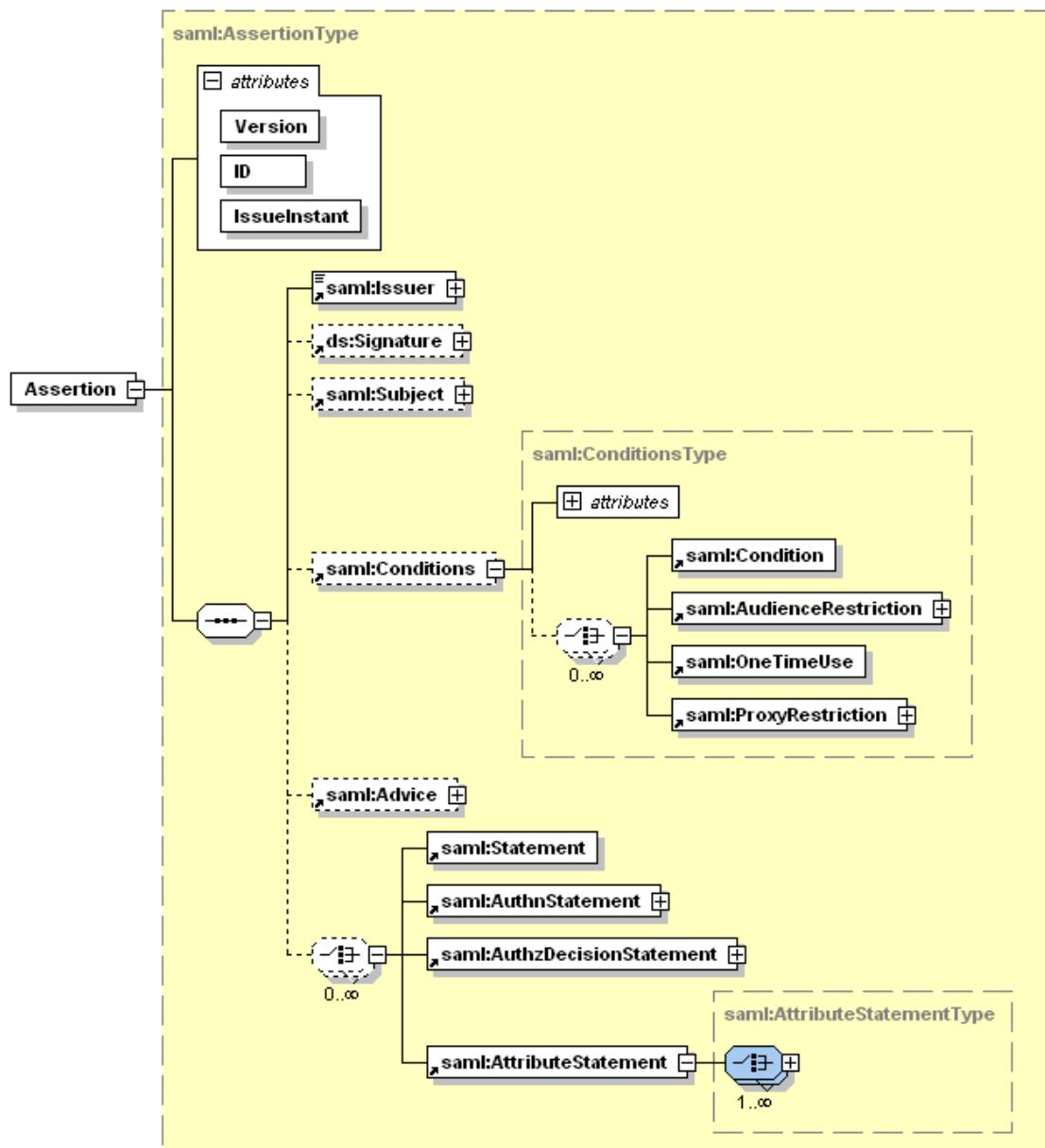


Figure: Identity Assertion – Top Level Elements of a SAML Assertion

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Assertion Element		Opt	Usage Convention
@Version		R	MUST be "2.0"
@ID		R	URN encoded unique identifier (UUID) of the assertion
@IssueInstant		R	time instant of issuance in UTC
Issuer		R	address URI that identifies the endpoint of the issuing service
Subject		R	
	NameID	R	Identifier of the HP encoded as an X.509 subject name, an e-Mail address or as a string value (unspecified format). NCP-B MUST guarantee that this identifier can be long-term tracked back to an individual person.
	@Format	R	MUST be "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" or "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName" or "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
	SubjectConfirmation	R	
	@Method	R	MUST be "urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"
	SubjectConfirmationData	X	
Conditions		R	
	@NotBefore	R	time instant from which the assertion is useable. This condition MUST be assessed to proof the validity of the assertion.
	@NotOnOrAfter	R	time instant at which the assertion expires. This condition MUST be assessed to proof the validity of the assertion. The maximum validity timespan for an HCP Identity Assertion MUST NOT be more than 4

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

			hours.
	AuthnStatement	R	
	@AuthnInstant	R	time instant of authentication in UTC
	@SessionNotOnOrAfter	O	Time instant of the expiration of the session
	AuthnContext	R	
	AuthnContextClassRef	R	Reference to the HP authentication method. See OASIS SAML Authn for a list of valid authentication methods.
	AttributeStatement	R	HP identity attributes and permissions (see e1-REQ-1906 and e1-REQ-1907)
	ds:Signature	R	Enveloped XML signature of the issuer of the HCP Identity Assertion (see e1-REQ-1905).

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.3.1.4.4 e1-REQ-1905 Assertion Signature

Every HCP Identity Assertion MUST be signed by its issuer. The XML signature MUST be applied by using the *saml:Assertion/ds:Signature* element as defined below.

Signature Parameter	Usage Convention
CanonicalizationMethod	SHOULD be "http://www.w3.org/2001/10/xml-exc-c14n#"
Transformation	Enveloped signature transform acc. to section 6.6.4 of W3C XMLDSig SHOULD be used (" http://www.w3.org/2000/09/xmldsig#enveloped-signature "). In addition, exclusive canonicalization SHOULD be defined as transformation (" http://www.w3.org/2001/10/xml-exc-c14n# ", acc. W3C XMLDSig and W3C XML-EXC 1.0). As inclusive namespaces other prefixes than the ones defined in e1-REQ-4874 of this document MUST NOT be used.
SignatureMethod	The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see e1-REQ-4877). For signing assertions the signature method " http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 " or " http://www.w3.org/2000/09/xmldsig#rsa-sha1 " SHOULD be used. A country MAY reject signatures that use SHA-1 for digesting.
DigestMethod	The hash algorithm MUST comply with the epSOS recommendations on algorithms and key lengths (see e1-REQ-4877). For signing assertions the digest method " http://www.w3.org/2000/09/xmldsig#sha1 " http://www.w3.org/2001/04/xmlenc#sha256 SHOULD be used. A country MAY reject SHA-1 digests.
KeyInfo	This element MUST either contain a wsse:SecurityTokenReference element which references the X.509 certificate of the assertion's issuer by using a subject key identifier OR contain a ds:X509Data

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

element which contains the X.509 certificate of the assertion issuer.

2.3.1.4.5 e1-REQ-1906 HCP Identity Attributes

An identity assertion can carry an arbitrary number of attributes on the authenticated entity.

Each attribute MUST be encoded using a SAML *attribute* element.

For epSOS the following attribute names and catalogues are defined.

HCP Identifier	
FriendlyName:	XSPA Subject
Name:	urn:oasis:names:tc:xacml:1.0:subject:subject-id
Values:	Human readable name of the HP
Type	String
Optionality:	Mandatory
Description:	This attribute MUST contain the full name of the HP.
Structural Role of the HCP	
FriendlyName:	XSPA Role
Name:	urn:oasis:names:tc:xacml:2.0:subject:role
Values:	See ASTM E1986-98 (2005). Only the ASTM structural roles “dentist”, “nurse” “pharmacist”, “physician”, “nurse midwife”, “admission clerk”, “ancillary services” and “clinical services” MUST be used.
Type	String
Optionality:	Mandatory
Speciality of the HCP	
FriendlyName:	HITSP Clinical Speciality
Name:	urn:epsos:names:wp3.4:subject:clinical-speciality
Values:	SNOMED CT based value set 2.16.840.1.113883.3.88.12.80.72 as defined in HITSP C80 2.0. See table 2-149 in HITSP C80 2.0 for the full list of

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

<p>possible values.</p> <p>Type: String</p> <p>Optionality: Optional</p>	
<p>Permissions acc. to the legislation of the country of care (country B)</p>	
<p>FriendlyName: XSPA permissions according with HI7</p> <p>Name: urn:oasis:names:tc:xspa:1.0:subject:hl7:permission</p> <p>Values: See e1-REQ-1907</p> <p>Type: URI</p> <p>Optionality: Optional. If no permissions are given, only the permissions of the HP structural role acc. to the legislation of the country of affiliation (country A) are considered for the access control decision. If permissions are defines, the country of affiliation SHOULD consider these for all access control decisions.</p>	
<p>Delegated Rights</p>	
<p>FriendlyName: OnBehalfOf</p> <p>Name: urn:epsos:names:wp3.4:subject:on-behalf-of</p> <p>Values: See ASTM E1986-98 (2005). Acc. to D3.6.2 only the ASTM structural roles “dentist”, “nurse” “pharmacist”, “physician” and “nurse midwife” MUST be used.</p> <p>Type: String</p> <p>Optionality: Mandatory if a structural role of “ancillary services” or “clinical services” is presented. For all other structural roles this attribute is optional</p> <p>Description: If a person is acting on behalf of another person the role of this person MAY be provided with this attribute. If this attribute is included with a HCP identity assertion, the issuer of the assertion MUST be able to track back the delegation to the two natural persons involved. Only valid roles as defined for HP structural roles MUST be used. A service provider MAY decide not to accept delegated access rights by just ignoring this attribute.</p>	
<p>Healthcare Professional Organisation</p>	

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

FriendlyName:	XSPA Organization
Name:	urn:oasis:names:tc:xspa:1.0:subject:organization
Values:	Name of the Healthcare Professional Organisation
Type:	String
Optionality:	Optional
Description	This value SHOULD only be provided if different from the point of care (e.g. in cases where a hospital organization runs multiple points of care or where a hospital just provides a professional environment for otherwise independent care providers)
Healthcare Professional Organisation ID	
FriendlyName:	XSPA Organization Id
Name:	urn:oasis:names:tc:xspa:1.0:subject:organization-id
Values:	URN encoded OID of the Healthcare Professional Organisation
Type:	URI
Optionality:	Optional
Type of HCPO	
FriendlyName:	epSOS Healthcare Facility Type
Name:	urn:epsos:names:wp3.4:subject:healthcare-facility-type
Values:	epSOS code list 1.3.6.1.4.1.12559.11.10.1.3.2.2.2 as defined in e1-REQ-4875 [1]. Possible values are: "Hospital", "Resident Physician", "Pharmacy", "Other".
Type:	String
Optionality:	Mandatory
Description	If a healthcare facility is not operated under the supervision of a physician or pharmacist the healthcare facility type MUST be set to "Other".
Purpose of Use	
FriendlyName:	XSPA Purpose of Use

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Name:	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse
Values:	For epSOS only TREATMENT (healthcare facility) and EMERGENCY (emergency department, ambulance, etc.) are allowed as purpose of use. If a HP requests claims for another purpose of use, the request must be rejected as unauthorized.
Optionality:	Mandatory
Description	As the HCP identity assertion is independent of a specific patient's treatment, this attribute refers to the usual working environment of the user.
Point of Care	
Attribute Name:	XSPA Locality
Catalogue:	urn:oasis:names:tc:xspa:1.0:environment:locality
Values:	String
Optionality:	Mandatory
Description	Name of the hospital or medical facility where patient care takes place.

[1] A new catalogue had to be defined for epSOS because the SNOMED CT based value set 2.16.840.1.113883.3.88.12.80.67 as defined in HITSP C80 2.0 does not include codes for pharmacies and goes too much into detail wrt the requirements on HCPO type identification as expressed in D3.6.2.

Pilot projects MAY agree on further attributes. Nevertheless all attributes not listed in this list MAY be ignored by the service provider.

2.3.1.4.6 e1-TXT-745 Sample Assertion

Related to e1-REQ-1301 Sample Assertion

```
<soap12:Envelope ... >
<soap12:Header ... >
<wsse:Security ... >
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="urn:uuid:7102AC72154DCFD1F51253534608781"
```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

IssueInstant="2009-09-21T12:03:28.788Z" Version="2.0">

<saml:Issuer>**urn:idp:countryB**</saml:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />

<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />

<ds:Reference URI="#urn:uuid:7102AC72154DCFD1F51253534608780">

<ds:Transforms>

<ds:Transform

Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />

<ds:Transform

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

<ec:InclusiveNamespaces

xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"

PrefixList="ds saml xs" />

</ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

<ds:DigestValue>A1LyLvFHRrYaOJ28YVFd3MfKGSI=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>cH+ICY ... </ds:SignatureValue>

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate>MIIADS ... </ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</ds:Signature>

<saml:Subject>

<saml:NameID

Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">

Franz.Muller@AKH.Vienna.at

</saml:NameID>

<saml:SubjectConfirmation

Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">

<saml:SubjectConfirmationData/>

</saml:SubjectConfirmation>

</saml:Subject>

<saml:Conditions

NotBefore="**2009-09-21T12:03:28.788Z**"

NotOnOrAfter="**2009-09-21T16:03:28.788Z**">

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

</saml:Conditions>
<saml:AuthnStatement
AuthnInstant="2009-09-21T12:03:28.788Z"
SessionNotOnOrAfter="2009-09-21T16:03:28.788Z">
<saml:AuthnContext>
<saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:X509
</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute
FriendlyName="XSPA Subject"
Name="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Dr. Franz Muller
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
FriendlyName="XSPA Organization"
Name="urn:oasis:names:tc:xspa:1.0:subject:organization"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Vienna AKH
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
FriendlyName="XSPA Organization Id"
Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:anyURI">urn:oid:1.2.3.4.5.6.7
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

FriendlyName="epSOS Healthcare Facility Type"
Name=" urn:epsos:names:wp3.4:subject:healthcare-facility-type"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">Hospital
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
  FriendlyName="XSPA permissions according with HI7"
  Name="urn:oasis:names:tc:xspa:1.0:subject:hl7:permission"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">urn:oasis:names:tc:xspa:1.0:hl7:PRD-006
</saml:AttributeValue>
<saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">urn:oasis:names:tc:xspa:1.0:hl7:PRD-017
</saml:AttributeValue>
<saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">urn:oasis:names:tc:xspa:1.0:hl7:PRD-010
</saml:AttributeValue>
... See HI7 permission catalogue for further values that may be used
</saml:Attribute>
<saml:Attribute
  FriendlyName="XSPA Role"
  Name="urn:oasis:names:tc:xacml:2.0:subject:role"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">Physician
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
  FriendlyName="XSPA Purpose of Use"

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

```

Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">TREATMENT
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
FriendlyName="XSPA Locality"
Name="urn:oasis:names:tc:xspa:1.0:environment:locality"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">vienna-akh
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</wsse:Security>
```

2.3.1.4.7 e1-REQ-1902 Treatment Relationship Confirmation Assertion

Related to e1-REQ-1981 HP-B Identification and Authentication

Related to e1-REQ-4877 Cryptographic Keys and Algorithms

2.3.1.4.8 e1-TXT-747 Note

The Treatment Relationship Confirmation Assertion is a profiled SAML v2.0 assertion. It attests the existence of a treatment relationship between a patient and a HPO and provides information about the context of a certain treatment scenario.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.4.9 e1-REQ-1909 Generic Structure of the Treatment Relationship Assertion

The epSOS Confirmation Assertion is encoded as a SAML 2.0 assertion. The following restrictions and recommendations apply:

Assertion Element	Op t	Usage Convention
@Version	R	MUST be "2.0"
@ID	R	URN encoded unique identifier (UUID) of the assertion
@IssueInstant	R	time instant of issuance in UTC
Issuer	R	address URI that identifies the endpoint of the issuing service
Subject	R	
NameID	R	Identifier of the HCP encoded as an X.509 subject name, an e-Mail address or as a string value (unspecified format). The same identifier and encoding MUST be used as for the referenced HCP Identity Assertion.
@Format	R	MUST be "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" or "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName" or "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
SubjectConfirmation	R	
@Method	R	MUST be "urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"
Conditions	R	
@NotBefore	R	time instant from which the assertion is useable. This condition MUST be assessed to proof the validity of the assertion.
@NotOnOrAfter	R	time instant at which the assertion expires. This condition

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

		MUST be assessed to proof the validity of the assertion. The maximum validity timespan for a Treatment Relationship Confirmation Assertion MUST NOT be more than 2 hours.
Advice	R	
AssertionIdRef	R	Reference to the HCP identity assertion that provides information on the HCP and the healthcare facility that were authorised by the patient to access his medical data
AuthnStatement	R	
@AuthnInstant	R	time instant of authentication in UTC
@SessionNotOnOrAfter	O	Time instant of the expiration of the session
AuthnContext	R	
AuthnContextClassRef	R	MUST be "urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
AttributeStatement	R	Patient identity attributes and treatment context information (see e1-REQ-1911)
ds:Signature	R	Signature of the issuer of the Treatment Relationship Conformation Assertion (see e1-REQ-1910).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.4.10 e1-REQ-1910 Assertion Signature

Every Treatment Relationship Confirmation Assertion MUST be signed by its issuer. The XML signature MUST be applied by using the *saml:Assertion/ds:Signature* element as defined below

Signature Parameter	Usage Convention
CanonicalizationMethod	SHOULD be "http://www.w3.org/2001/10/xml-exc-c14n#"
Transformation	Enveloped signature transform acc. to section 6.6.4 of W3C XMLDSig SHOULD be used (http://www.w3.org/2000/09/xmldsig#enveloped-signature). In addition, exclusive canonicalization SHOULD be defined as transformation (http://www.w3.org/2001/10/xml-exc-c14n#), acc. W3C XMLDSig and W3C XML-EXC 1.0). As inclusive namespaces other prefixes than the ones defined in e1-REQ-4874 MUST NOT be used.
SignatureMethod	The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see e1-REQ-4877). For signing assertions the signature method http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 or http://www.w3.org/2000/09/xmldsig#rsa-sha1 SHOULD be used. A country MAY reject signatures that use SHA-1 for digesting.
DigestMethod	The hash algorithm MUST comply with the epSOS recommendations on algorithms and key lengths (e1-REQ-4877). For signing assertions the digest method http://www.w3.org/2000/09/xmldsig#sha1 http://www.w3.org/2001/04/xmlenc#sha256 SHOULD be used. A country MAY reject SHA-1 digests.
KeyInfo	This element MUST either contain a wsse:SecurityTokenReference element which references the X.509 certificate of the assertion's issuer by using a subject key identifier OR contain a ds:X509 Data element which contains the X.509 certificate of the assertion issuer.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.3.1.4.11 e1-REQ-1911 Patient Identity and Treatment Context Attributes

A Treatment Relationship Confirmation assertion can carry an arbitrary number of attributes on the identified patient and the current treatment context. Each attribute MUST be encoded using a SAML *attribute* element.

For epSOS the following attribute names and catalogues are defined.

Patient Identifier	
FriendlyName:	XSPA subject
Name:	urn:oasis:names:tc:xacml:1.0:resource:resource-id
Values:	URI encoded identifier of the patient as obtained by the id traits handshake
Type	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
Optionality:	Mandatory
Purpose of Use	
FriendlyName:	XSPA Purpose Of Use
Name:	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse
Values:	For epSOS only TREATMENT (healthcare treatment) and EMERGENCY (emergency treatment) are allowed as purpose of use. If a request claims for another purpose of use, the request must be rejected as unauthorized.
Optionality:	Optional
Description	If this attribute is present, it overwrites the purpose of use attribute contained with the HCP identity assertion.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.3.1.4.12 e1-TXT-748 Sample Assertion

Related to e1-REQ-1306 Sample Assertion

```

<soap12:Envelope ... >
<soap12:Header ... >
<wsse:Security ... >
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="urn:uuid:7102AC72154DCFD1F51253534608781"
    IssueInstant="2009-09-21T12:03:28.788Z" Version="2.0">
<saml:Issuer>urn:idp:countryB</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<ds:Reference URI="#urn:uuid:7102AC72154DCFD1F51253534608780">
<ds:Transforms>
<ds:Transform
    Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform
    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ec:InclusiveNamespaces
    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
    PrefixList="ds saml xs" />
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>A1LyLvFHRrYaOJ28YVFd3MfKGSI=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>cH+ICY ... </ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIlADS ... </ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Franz.Muller@AKH.Vienna.at

```

</saml:NameID>
<saml:SubjectConfirmation
  Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
</saml:Subject>
<saml:Conditions
  NotBefore="2009-09-21T12:03:28.788Z"
  NotOnOrAfter="2009-09-21T14:03:28.788Z">
</saml:Conditions>
<Advice>
  <AssertionIdRef>urn:uuid:7102AC72154DCFD1F51253534608781</AssertionIdRef>
</Advice>
<saml:AuthnStatement
  AuthnInstant="2009-09-21T12:03:28.788Z"
  SessionNotOnOrAfter="2009-09-21T14:03:28.788Z">
<saml:AuthnContext>
<saml:AuthnContextClassRef>
  urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute
  FriendlyName="XSPA subject"
  Name="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">Patient ID
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
  FriendlyName="XSPA Purpose Of Use"
  Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">TREATMENT
</saml:AttributeValue>
</saml:Attribute>
```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

</saml:AttributeStatement>

</saml:Assertion>

2.3.1.4.13 e1-REQ-1913 Audit Trail Consideration

The NCP MUST write an audit trail entry for the confirmation of a treatment relationship (e. g. after the attesting signature has been applied to the Treatment Relationship Confirmation Assertion). The audit message MUST be assembled according to the HCP Assurance audit schema as defined in e1-REQ-1838.

The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event
Requesting Point of Care	R	HCPO which is in a treatment relationship with the patient
Human Requestor	R	HP who requested the confirmation of the treatment relationship
Source Gateway	R	Outbound gateway that attested the authenticity of the Treatment Relationship Confirmation Assertion
Target Gateway	X	
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	R	Patient who is in a treatment relationship with the HCPO
Event Target	X	

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.3.1.4.14 e1-REQ-1903 epSOS Certificate Profiles

Related to e1-REQ-4877 Cryptographic Keys and Algorithms

The following requirements define how to set up epSOS compliant X.509 certificates. All certificates issued by a CA that are used for epSOS are to be based on these guidelines.

epSOS compliant certificates SHOULD be Common PKI compatible.

The algorithms and key lengths used with epSOS compliant certificates MUST follow the “epSOS Cryptographic Keys and Algorithms” (see e1-REQ-4877)

Version

Certificates to be deployed MUST be v3.

Signature algorithm

“epSOS Cryptographic Keys and Algorithms” recommendations (see e1-REQ-4877) MUST be followed.

Serial number

The serial number MUST be an unambiguous positive integer value with a maximum of 20 bytes.

Validity from/to

Certificates used by epSOS services SHOULD be valid for a maximum of 1 year.

IssuerUniqueID

The field "IssuerUniqueID" MUST NOT be used.

SubjectUniqueID

The field "SubjectUniqueID" MUST NOT be used.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Subject

The Subject-DName MUST remain unambiguous over the entire lifetime of the CA.

The minimal attributes the DName MUST have are C (Country), O (Organization), and CN (Common Name).

The attributes T (Title), G (Given Name), and SN (Surname), containing information about the authority responsible for the certificate, SHOULD be used. The attribute OU (Organizational Unit) MAY be used.

String lengths MUST be limited as follows:

- C (Country)→ 2 bytes (ISO 3166 code)
- O (Organization)→ max. 64 bytes
- CN (Common Name)→ max. 64 bytes
- T (Title)→ max. 64 bytes
- G (Given Name)→ max. 64 byte
- SN (Surname)→ max. 64 bytes
- OU (Organizational Unit)→ max. 64

Further DName attributes (for example E (E-Mail)) SHOULD NOT be provided. If, however, they are deployed, the Common PKI string-length limits MUST be adhered to.

The DName string MUST be coded in UTF8. The use of a subset (Unicode Latin-1 page - ANSI/ISO 8859-1) is recommended (SHOULD).

The certificate SHOULD always include the name of a contact person:

C=[Country Code], O=[Name of the Organisation](, OU=[Organizational Unit]), CN= [Common Name, T=[Title], G=[Contact person's given name(s)], SN=[Contact person's surname(s)]

Issuer

The DName must be identical to the subject DName of the Issuer certificate. [MUST]

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.3.1.4.15 e1-REQ-1915 Certificate Profile - Certificate Extensions

The following section discusses X.509v3 certificate extensions, which must be considered in the present specification. The structuring is based strictly on the Common PKI standard.

In addition to the extensions presented here, others may be included, but they must be in strict compliance with the Common PKI specification. Limiting the extensions selected to those delineated here is recommended.

AuthorityKeyIdentifier (non-critical)

"Authority KeyIdentifier" MUST be included as an extension in the certificate.

The "SubjectKeyIdentifier" of the issuing CA MUST be used.

AuthorityCertIssuer and AuthorityCertSerialNumber SHOULD NOT be used as AuthorityKeyIdentifier.

SubjectKeyIdentifier (non-critical)

"SubjectKeyIdentifier" MUST be included as an extension in the certificate.

One of the methods described in RFC5280 (ch. 4.2.1.2) SHOULD be used.

KeyUsage (critical)

"KeyUsage" MUST be included as an extension in the certificate.

The extension MUST always be designated as critical.

The usage type is specific for each epSOS certificate profile (see following requirements)

IssuerAltNames (non-critical)

"IssuerAltNames" MAY be included as an extension in the certificate.

If this extension is used, providing a corresponding LDAP-URL from which the issuer certificate can be called up is recommended. (SHOULD)

HTTP and FTP URLs that refer to the certificate MAY also be provided.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

SubjectAltNames (non-critical)

"SubjectAltNames" MAY be included as an extension in the certificate.

If this extension is used, providing a corresponding LDAP-URL from which the issuer certificate can be called up is recommended. (SHOULD)

HTTP and FTP URLs that refer to the certificate MAY also be provided.

E-Mail addresses (RFC822-name) MAY also be made available.

BasicConstraints (critical)

"BasicConstraints" MUST be included as an extension in the certificate.

The extension MUST always be designated as critical.

The extension MUST assume the value FALSE for "ca".

ExtendedKeyUsage (non critical)

The use of this attribute is specific for each epSOS certificate profile (see following requirements)

CRLDistributionPoints (non-critical)

"CRLDistributionPoints" SHOULD be included as an extension in the certificate.

This extension SHOULD include the HTTP address from which the certificate-issuing authority's complete revocation list can be retrieved.

Optionally, URLs (also LDAP and FTP) where the CRL can be retrieved MAY also be indicated. No other information may be included in the extension.

CertificatePolicies (non-critical)

"CertificatePolicies" SHOULD be included as an extension in the certificate.

Policyinformation SHOULD **only** include an OID.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Authority Info Access (non-critical)

"AuthorityInfoAccess" SHOULD be included as an extension in the certificate.

When the issuing CA offers an OCSP service, its HTTP URI MUST be included in the extension.

Even though AuthorityInfoAccess and CRLDistributionPoints are specified as non-mandatory extensions, one of them MUST be included in the certificate as defined above.

2.3.1.4.16 e1-REQ-1916 Certificate Profile: VPN Client Gateway Authenticity

The following constraints are specific for epSOS IPsec Client certificates.

KeyUsage (critical)

For IPsec client certificates, only the "digitalSignature" usage type MUST be specified.

ExtendedKeyUsage (non critical)

"ExtendedKeyUsage" SHOULD be included as an extension in the certificate.

If this extension is included in the certificate, it MUST only accept the value "ClientAuth" (OID 1.3.6.1.5.5.7.3.2).

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.3.1.4.17 e1-REQ-1917 Certificate Profile: VPN Server Gateway Authenticity

The following constraints are specific for epSOS IPSec Server certificates.

Subject

Server certificates are used for the authentication of servers/services, and this MUST be considered in the Subject when defining the "Distinguished Name".

The certificate SHOULD always include the name of a contact person.

The CN (Common Name) MUST include the DNS server name; if it doesn't, the client's default setting identifies the server certificate as untrustworthy.

KeyUsage (critical)

For VPN server certificates, only the "keyEncipherment" usage type MUST be specified.

ExtendedKeyUsage (non critical)

"ExtendedKeyUsage" SHOULD be included as an extension in the certificate.

If this extension is included in the certificate, it MUST only accept the value "ServerAuth" (OID 1.3.6.1.5.5.7.3.1).

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.3.1.4.18 e1-REQ-1918 Certificate Profile: Service Consumer Node Authenticity

The following constraints are specific for epSOS SSL Client certificates.

KeyUsage (critical)

For SSL client certificates, only the "digitalSignature" usage type MUST be specified.

ExtendedKeyUsage (non critical)

"ExtendedKeyUsage" SHOULD be included as an extension in the certificate.

If this extension is included in the certificate, it MUST only accept the value "ClientAuth" (OID 1.3.6.1.5.5.7.3.2).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.4.19 e1-REQ-1919 Certificate Profile: Service Provider Node Authenticity

The following constraints are specific for epSOS SSL Server certificates.

Subject

Server certificates are used for the authentication of servers/services, and this MUST be considered in the Subject when defining the "Distinguished Name".

The certificate SHOULD always include the name of a contact person.

The CN (Common Name) MUST include the DNS server name; if it doesn't, the client's default setting identifies the server certificate as untrustworthy.

KeyUsage (critical)

For SSL server certificates, **only** the "keyEncipherment" usage type MUST be specified.

ExtendedKeyUsage (non critical)

"ExtendedKeyUsage" SHOULD be included as an extension in the certificate.

If this extension is included in the certificate, it MUST **only** accept the value "ServerAuth" (OID 1.3.6.1.5.5.7.3.1).

2.3.1.4.20 e1-REQ-1920 Certificate Profile: NCP Signature

The following constraints are specific for epSOS NCP signature certificates.

KeyUsage (critical)

Only the "digitalSignature" AND "nonRepudiation" usage type MUST be specified.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

ExtendedKeyUsage (non critical)

"ExtendedKeyUsage" MUST NOT be included as an extension in the certificate.

2.3.1.4.21 e1-REQ-1921 Certificate Profile: OCSP Responder Certificates

The following constraints are specific for epSOS OCSP Responder certificates.

KeyUsage (critical)

Only the "nonRepudiation" usage type MUST be specified.

ExtendedKeyUsage (non critical)

"ExtendedKeyUsage" SHOULD be included as an extension in the certificate.

If this extension is included in the certificate, it MUST only accept the value „id-kp-OCSPSigning“ (OID 1.3.6.1.5.5.7.3.9)

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.4.22 e1-REQ-1922 Certificate Profile: Certificate Revocation Lists

The following requirements define the profile (structure) of a CRL, and all CRLs issued by the CA are to be based on these guidelines. The following requirements refer to direct CRLs.

CRLs MUST be Common PKI compatible.

Version

CRLs to be deployed MUST be v2.

Signature algorithm

See “epSOS Cryptographic Keys and Algorithms” recommendations (e1-REQ-4877).

Issuer

The DName MUST be identical to the subject DName of the issuer certificate.

Validity from/to (thisUpdate/nextUpdate)

The CRL’s period of validity (from/to) MUST be stated.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.4.23 e1-REQ-1924 CRL Profile - CRL Extensions

Like certificates, CRLs can also have extensions, some options for which are provided in the following section.

Others are also possible, but it is mandatory that any CRL extension used be compatible with the Common PKI specification. It is recommended that only the extensions presented here be employed.

AuthorityKeyIdentifier

The KeyIdentifier MUST be indicated.

CRLNumber

The consecutive number for the CRL issued MUST be indicated.

It MUST have a unique positive integer value with a maximum length of 20 bytes.

IssuerAltNames

"IssuerAltNames" MAY be an extension in the CRL.

When using the extension, it is recommended that a corresponding LDAP-URL be given with which the issuer certificate can be obtained (SHOULD).

HTTP and FTP URLs that refer to the certificate MAY also be provided.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.3.1.4.24 e1-TXT-750 Note

CRLs can be used to check whether a certificate has been declared invalid or revoked. Both the client and server/service have to reciprocally authenticate all certificates against the CRL before transmitting data to the counterpart. If the certificate is invalid, the connection is terminated.

2.3.1.5 e1-REQ-4860 Exception Handling

Related to e1-REQ-4847 Error Handling

Related to e1-REQ-4859 Expected Actions

Related to e1-REQ-4895 Expected Actions

Related to e1-REQ-4908 Expected Actions

Related to e1-REQ-4918 Expected Actions

Related to e1-REQ-4927 Expected Actions

Related to e1-REQ-4934 Expected Actions

Related to e1-REQ-4944 Expected Actions

Related to e1-REQ-4848 SOAP Faults

2.3.1.5.1 e1-REQ-4861 Communication Failures and Audit Trail

Communication failures are raised by the existing mechanisms of the communication and messaging protocols. They are handled on the layer where they occurred. epSOS does not define new error codes for these kinds of failures and epSOS does not define any requirements for raising and processing these errors that are beyond the presetting of the respective standards. This includes that errors of this kind can occur at both communicating gateways and MAY require action to be taken by both gateways.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.3.1.5.2 e1-REQ-4862 Audit Trail to be generated by NCP-B

Related to e1-REQ-4622 REQ 3.3.30 Logging of errors

In case of a communication failure an audit trail entry MUST be written at NCP-B:

epSOS Instance	Opt.	Description
Event	R	Service that was to be called
Requesting Point of Care	R	HPO that issued the original request.
Human Requestor	R	HP that triggered the request
Source Gateway	R	Service consumer node address at the country of Care
Target Gateway	R	Service provider node that did not respond to the request
Audit Source	X	-
Patient	R	Patient
Event Target	X	-
Error Message	R	Error data as provided by the layer that detected the communication failure

2.3.1.5.3 e1-REQ-4863 Encoding and Consistency Failures

Encoding and consistency problems SHOULD be detected at the protocol terminator or other epSOS-side internal components at the service providing NCP. Errors that origin in an improper encoding of the message (envelope, header) or in an inaccurate use of security objects are covered by the SOAP error mechanism.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.3.1.5.4 e1-REQ-4864 SOAP Error Profile

Information on faults that occurred during the processing of a request are placed into a SOAP response message body as SOAP 1.2 faults. The respective data type MUST be instantiated as defined in W3C SOAP 1.2. epSOS specific error information is encoded with the following elements:

Element name	Format	Opt.	Content
Code/Subcode/Value	QName	R	epSOS error code
Reason/Text	QName	R	Description of the error (by default the error code is used as the error description; nevertheless a NCP implementation MAY provide the error condition or even more detailed information on the reason of the failure in this element)
Node	URI	O	URI of the system component that caused the failure or (URI encoded) OID of the object that caused the error. The semantics of this entry MUST be determinable by the error code. By default this element holds the URI of the Service Provider where the error was detected.

Further details on the error MAY be given in a <detail/> element. The receiver of the fault message MUST NOT process the <detail/> element but SHOULD dump its contents into the respective field of the audit trail entry.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

2.3.1.5.5 e1-REQ-4865 General Message Handling Errors

The following table lists all general message handling errors. These errors MUST be handled acc. to the epSOS SOAP error profile.

Condition	Code	Subcode	Action to be taken
The service provider is not able to fulfil the request due to an internal problem	Receiver	Busy	Both NCPs MUST write an audit trail entry. The service requestor SHOULD send the request again.
The service provider cannot write an audit trail entry.	Receiver	Audit Log Failure	The service consumer MUST write an audit trail entry. The service provider MUST write a log entry to the systems log. The system administrator MUST process this failure because it indicates a mis-configuration or software error.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.5.6 e1-REQ-4866 SOAP Message Encoding and Addressing Errors

The following table lists all message encoding and addressing errors. These errors MUST be handled acc. to the epSOS SOAP error profile.

Condition	Code	Subcode	Action to be taken
The protocol terminator cannot decode the message because of a schema violation in the SOAP envelope	MustUnderstand or DataEncodingUnknown (depending on the source of the error)	Decoding Failure	No audit trails are written. The service consumer MUST write a log entry to the systems log. The system administrator MUST process this failure because it indicates a mis-configuration or software error.
The protocol terminator cannot validate a message because of an unknown namespace or schema	DataEncodingUnknown	Unknown Schema	No audit trails are written. The service consumer MUST write a log entry to the systems log. The system administrator MUST process this failure because it indicates a mis-configuration or software error.
The protocol terminator cannot process the message because it does not know or not support the requested service.	MustUnderstand or DataEncodingUnknown (depending on the source of the error)	Unknown Transaction	No audit trails are written. The service consumer MUST write a log entry to the systems log. The system administrator MUST process this failure because it indicates a mis-configuration or software error.
The protocol terminator rejects the message because of a version mismatch (e. g. service consumer uses deprecated version of	MustUnderstand or DataEncodingUnknown (depending on the source of the error)	Version Mismatch	No audit trails are written. The service consumer MUST write a log entry to the systems log. The system administrator MUST process this failure because it indicates a mis-configuration or software

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

the spec)			error.
-----------	--	--	--------

2.3.1.5.7 e1-REQ-4867 Security Header Encoding and Consistency Errors

The following table lists all security header related errors. These errors MUST be handled acc. to the epSOS SOAP error profile.

Condition	Code	Subcode	Action to be taken
The provided HCP Identity Assertion does not contain all of the required attributes.	Sender	HCP Missing Attributes	Both service consumer and service provider MUST write an audit trail entry. The service consumer SHOULD request a new authentication of the HP.
The provided HCP Identity Assertion is not valid or timed out.	Sender	Invalid Security Token	Both service consumer and service provider MUST write an audit trail entry. The service consumer SHOULD request a new HP authentication.
The patient identifier is not valid.	Sender	Unknown Patient	Both service consumer and service provider MUST write an audit trail entry. The HP at the country of care SHOULD identify the patient again, establish a new security context and retry the request.
An attesting (message) signature cannot be verified.	Sender or Receiver (depending on the source of the failure)	Invalid NCP Signature	Both service consumer and service provider MUST write an audit trail entry. The service provider MUST write a log entry to the systems log. The system administrator MUST process this failure because it indicates a mis-configuration or software error.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

The use of SHA-1 as a digesting method is not allowed.	Sender or Receiver (depending on the source of the failure)	Weak Digest	Both service consumer and service provider MUST write an audit trail entry. The service provider MUST write a log entry to the systems log. The service consumer SHOULD re-issue the request using SHA-2 for digesting (message signature and assertion signatures). The service provider SHOULD use the same digesting method for message signatures as the service consumer.
The requestor provided a Confirmation Assertion which is not accepted by the service provider.	Sender	Weak Authorisation	Both service consumer and service provider MUST write an audit trail entry. The HP SHOULD trigger the issuance of a new TRC assertion by NCP-B and re-issue the request.

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version: 1.0
D5.2.3	Date: 31/01/2013

2.3.1.5.8 e1-REQ-4868 Audit Trail Considerations by NCP-A & NCP-B

Related to e1-REQ-4622 REQ 3.3.30 Logging of errors

In case of a general message handling error, NCP-B MUST write a full audit trail including a defined error section as defined in e1-REQ-1838.

NCP-A MUST fill all audit trail information that could be decoded from the request message. If the requested operation cannot be decoded the Event Identification section of the HCP Assurance Audit Schema MUST be used as follows:

Field Name	Value Constraints
EventID	MUST be set to EV(epsos-00, "unknown", unknown)
EventActionCode	MUST be set to E (execute).
EventDateTime	Time of the occurrence of the failure
EventOutcomeIndicator	Acc. RFC 3881. MUST be "4" for temporal or recoverable failures and "8" for permanent failures.

If the HP identity cannot be decoded from the HCP Identity Assertion, the Human Requestor section of the HCP Assurance Audit Schema MUST be used as follows:

Field Name	Value Constraints
UserID	Subject and issuer MUST be set to "unknown". See e1-REQ-1878 for the mandatory encoding scheme for user identifiers.
UserName	MUST be set to "unknown"
UserIsRequestor	"true"
RoleIDCode	MUST be omitted.

If the patient identity cannot be decoded from the request, the Patient section of the HCP Assurance Audit Schema MUST be used as follows:

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Field Name	Value Constraints
ParticipantObjectTypeCode	MUST be "1" (Person)
ParticipantObjectTypeCodeRole	MUST be "1" (Patient)
ParticipantObjectIDTypeCode	EV(2, RFC-3881, "Patient Number")
ParticipantObjectID	MUST be "unknown"

2.3.1.6 e1-REQ-4874 Namespaces

XML namespace prefixes stand for their respective namespaces as follows:

Prefix	Namespace
epsos	urn:epsos:v1
soapenv	http://www.w3.org/2003/05/soap-envelope
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
saml	urn:oasis:names:tc:SAML:1.0:assertion
xacml	urn:oasis:names:tc:xacml:2.0:policy:schema:os
hl7v2	urn:hl7-org:v2
hl7v3	urn:hl7-org:v3
xds	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

rimext	urn:ihe:iti:xds-ebrim:extensions:2010
query	urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0
rim	urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0
rs	urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0
lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0
tsl	http://uri.etsi.org/02231/v2#

2.3.1.7 e1-FLD -276 epSOS Identifiers

2.3.1.7.1 e1-REQ-5268 epSOS WP3.4 Uniform Resource Names (URNs)

For epSOS WP3.4 the following URNs are defined:

URN	Description
urn:epsos:names:wp3.4:subject:healthcare-facility-type	Signals that a SAML attribute refers to the kind of the healthcare facility assigned to the subject. See e1-REQ-1906 for details.
urn:epsos:names:wp3.4:subject:clinical-speciality	Signals that a SAML attribute refers to the kind of the clinical speciality of the subject. See e1-REQ-1906 for details.
urn:epsos:names:wp3.4:subject:on-behalf-of	Signals that a SAML attribute refers to the person who authorized the subject's access to epSOS services. See e1-REQ-1906 for details.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.7.2 e1-REQ-5269 epSOS OIDS

In the absence of an official epSOS OID [ISO OID] a temporary OID is assigned as the root OID 1.3.6.1.4.1.12559.11.10.1.3 for epSOS. Branch 2 was allocated to WP3.4; therefore the root OID for objects belonging to WP3.4 is 1.3.6.1.4.1.12559.11.10.1.3.2.

The following branches are defined for WP3.4 codes and code systems:

OID Branch	Description
1.3.6.1.4.1.12559.11.10.1.3.2.2	Patient Identification related codes and code systems
1.3.6.1.4.1.12559.11.10.1.3.2.2	HCP(O) identification, authentication, authorisation related codes and code systems
1.3.6.1.4.1.12559.11.10.1.3.2.3	Medical data sharing related codes and code systems
1.3.6.1.4.1.12559.11.10.1.3.2.4	Consent encoding and management related codes and code systems

For epSOS Common Components Specification (WP 3.4) the following OIDs are defined:

OID	Type	Values / Description
1.3.6.1.4.1.12559.11.10.1.3.2.2.1	Code list	{“AdditionalDemographicsRequested”, “DemographicsQueryNotAllowed”, “EHICDataRequested”, “InsufficientRights”, “PrivacyViolation”, “AnswerNotAvailable”, “PolicyViolation”, “PatientAuthenticationRequired” }
1.3.6.1.4.1.12559.11.10.1.3.2.2.2	Code list	{“Hospital”, “Resident Physician”, “Pharmacy”, “Other” }
1.3.6.1.4.1.12559.11.10.1.3.2.3.1	Code list	{ “epSOS pivot” }
1.3.6.1.4.1.12559.11.10.1.3.2.4.1	Coded values	1: Opt-In Policy 2: Opt-Out Policy

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

2.3.1.7.3 E1-REQ-5270 epSOS WP3.4 CDA Documents and Codes

epSOS Consumer Document	Display Name	Coding Scheme	Node Representation
Patient Summary	Patient Summary	2.16.840.1.113883.6.1	60591-5
eDispensation	eDispensation	2.16.840.1.113883.6.1	60593-1
ePrescription	ePrescription	2.16.840.1.113883.6.1	57833-6
Consent	Privacy Policy Acknowledgement Document	2.16.840.1.113883.6.1	57016-8

2.3.1.8 e1-REQ-1907 Use of HL7 Permission Codes

The epSOS access control paradigm follows the “needs to know” principle by respecting the role and task definitions and derived permissions that a HP is assigned in the country of care. As these permissions can only be defined and assigned by the HPs local legal context, they are transmitted to the patient’s country of affiliation as part of the HCP identity assertion. For the recently defined epSOS use cases the following permission codes as defined in the context of HL7’s role engineering are of interest:

Permission	Description
POE-006	Change/Discontinue/Refill Outpatient Prescription Order
PRD-003	Review Medical History
PRD-004	Review Existing Orders
PRD-005	Review Vital Signs/Patient Measurements
PRD-006	Patient Identification and Lookup
PRD-010	Review Patient Medications
PRD-016	Review Problem List
PPD-032	New Consents and Authorizations
PPD-033	Edit/Addend/Sign Consents and Authorizations
PPD-046	Record Medication Administration Record

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The following matrix shows which permissions MUST at least be assigned to an HP in order to perform the defined epSOS operations.

epSOS Service	Operation	Minimum Permissions
PatientIdentification Service	FindIdentityByTraits	PRD-006
Patient Service	List	PRD-003 and PRD-005 and PRD-010 and PRD-016
Order Service	List	PRD-004 and PRD-010
Dispensation Service	Initialize	PPD-046
	Discard	POE-006
Consent Service	Put	PPD-032
	Discard	PPD-033

2.3.1.9 e1-REQ-4877 Cryptographic Keys and Algorithms

Related to e1-REQ-1903 epSOS Certificate Profiles

Related to e1-REQ-1901 HCP Identity Assertion

Related to e1-REQ-1880 IPsec Configuration

Related to e1-REQ-4884 Message Signature

Related to e1-REQ-1881 TLS configuration

Related to e1-REQ-1902 Treatment Relationship Confirmation Assertion

All cryptographic keys and algorithms used for epSOS and its implementations MUST fulfil at least the requirements of ECRYPT-II D.SPA.57 for Level-5 (Legacy Standard) security. This corresponds to 96-bit security (symmetric equivalent).

The use of the 112-bit equivalent Level-6 (Medium Term Protection) security is recommended (SHOULD) for message security.

The use of the 128-bit equivalent Level-7 (Long Term Protection) security is recommended (SHOULD) for data security and digital certificates.

ECRYPT-II D.SPA.57 recommendations define the epSOS minimum requirements on the

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

selection of cryptographic keys and algorithms. Countries participating in and epSOS circle of trust MAY agree to choose another algorithm catalogue (e. g. BSI TR-3116, FNISA CryptMech, NIST SP800.57/1] as long as this does not fall behind ECRYPT-II D.SPA.57 Level-5.

Algorithms based on elliptic curves MAY be used if agreed by all countries that participate in the respective circle of trust. If SHA-2 is used, only non-patented hash algorithms of the SHA-2 family MUST be used (recommendation: SHA-256 (SHOULD)). SHA-1 MAY be used as a hash algorithm for the epSOS pilots, but a country MAY react to respective messages and security token with an error requesting SHA-2 to be used.

2.3.1.10 e1-REQ-4878 Country Codes

Fields carrying country code values MUST be coded in accordance with [ISO 3166-1] Alpha 2 codes.

Country Code (normative)	Home Community I.D. (informative)
AT	2.16.17.710.780
CZ	2.16.17.710.804
DE	2.16.17.710.803
DK	2.16.17.710.802
ES	2.16.17.710.801
FR	2.16.17.710.790
GR	2.16.17.710.808
IT	2.16.17.710.806
NL	2.16.17.710.810
SE	2.16.17.710.807
SK	2.16.17.710.805
TR	2.16.17.710.813
UK	2.16.17.710.809

The following exceptions apply:

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

For United Kingdom the country codes “GB” and “UK” are allowed.

For Greece the country codes “GR” and “EL” are allowed.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

2.3.2 e1-FLD-164 Computational Dimension

2.3.2.1 e1-REQ-1879 Trusted Node Infrastructure

Related to e1-REQ-1978 Data Integrity

Related to e1-REQ-4591 REQ 3.3.6 Secure Context Establishment

Related to e1-REQ-1222 Trusted Node Infrastructure

Related to e1-REQ-4885 Trusted Node Infrastructure

The mutual trust between a service consumer and a service provider is based on a mutually trusted, secure channel between the underlying network nodes.

The establishment of mutual trust between nodes is performed by:

IPSec, RFC 4301

Transport Layer Security v1.0[1], RFC 2246

IHE Audit Trail and Node Authentication, IHE ITI TF-2a August 2009

[1] epSOS will upgrade to TLS v1.2, RFC5246 as soon as stable implementations are available from industry and rolled out at the epSOS member states. For the first epSOS pilot phases the use of TLS v1.0 (implying SHA-1) seems sufficient as an additional level of protection is provided by the use of IPSec.

2.3.2.1.1 e1-REQ-1880 IPSec Configuration

Related to e1-REQ-4877 Cryptographic Keys and Algorithms

A gateway-to-gateway VPN MUST be set up between all epSOS nodes. IPSec ESP transport modus MUST be used. Perfect Forwarding Secrecy MUST be activated. SA Lifetime SHOULD be based on the number of exchanged packets and SHOULD NOT exceed 4GB.

Algorithms and key lengths MUST be used acc. to e1-REQ-4877. Gateway certificates MUST comply with the certificate profiles as defined in e1-REQ-1916 and e1-REQ-1917. The issuing certificate authorities (CAs) and all components and services for managing the lifecycle of the certificates must comply with the respective epSOS security policies (see epSOS D3.7.2).

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

2.3.2.1.2 e1-REQ-1881 TLS configuration

Related to e1-REQ-4877 Cryptographic Keys and Algorithms

All network nodes running epSOS service consumers or service providers MUST be implemented as IHE *Secure Node* actors acc. to the IHE ATNA profile. The establishment of mutual trust and the setup of the secure transport layer channel between two epSOS nodes are always initiated by a service consumer that connects to a service provider.

The messages for the establishment of the basic transport layer secure channel correspond to the TLS handshake protocol as profiled in the IHE ATNA Integration profile (transaction ITI-19 as specified in section 3.19 of IHE ITI TF 2a, August 2009).

With respect to the ITI-19 transaction specification the following constraints and extensions apply:

Algorithms and key lengths MUST be used acc. to e1-REQ-4877.

The node certificates MUST comply with the epSOS Node Authentication Certificate Profile (see e1-REQ-1918 and e1-REQ-1919 for the certificate profile specifications)

The issuing CA and all components and services for managing the lifecycle of the epSOS Node Authentication Certificates must comply with the respective epSOS security policies (see epSOS D3.7.2).

2.3.2.2 e1-REQ-1882 Time Synchronisation

Time synchronisation within the network of epSOS gateways is performed by:

Network Time Protocol (Version3) RFC 1305 as described in the

IHE Consistent Time Integration Profile IHE ITI TF-2a August 2009

Stratum 2 time servers (*Consistent Time Mediators*) SHOULD be operated by NCPs. All services that rely on consistent time within the epSOS Circle of Trust MUST be operated on a node that acts as a stratum 3 time server (*Consistent Time Consumer*). This in particular holds for

services that apply or verify digital signatures on messages, medical data or assertions,
services that contribute to the security audit trail.

epSOS time synchronisation for *Consistent Time Consumers* is handled by respective mechanisms of the underlying operating systems. The messages exchanged correspond to the NTP transactions described in detail in RFC 1305 and <http://www.ntp.org>. The underlying network protocol is UDP (port 123). Authentication MAY be enabled with the *ntp authenticate* command

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Consistent Time servers that represent a Stratum n+1 server SHOULD have a configuration with a default polling interval of 4096 seconds at a minimum in order to synchronize the epSOS reference time to all nodes. Following time servers SHOULD only configure a polling interval of 65536 seconds.

Each Consistent Time Mediator SHOULD accept a maximum clock skew of 256 seconds. With respect to lower the system resources (due to incoming requests) of the Consistent Time Source, Consistent Time Mediators SHOULD peer themselves.

2.3.2.3 e1-FLD-192 Access Control

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3 e1-FLD-28 Service specific Profile

3.1 e1-FLD-69 epSOS Semantic Implementation Guidelines

3.1.1 e1-FLD-193 Conceptual Perspective

3.1.2 e1-FLD-70 Logical Perspective

3.1.2.1 e1-REQ-3900 Original document identification

Related to e1-REQ-1988 Peering Original Document

Implemented by e1-REQ-2081 Implementable Original document identification

Countries receiving an epSOS record (e.g. epSOS pivot) SHALL be enabled to identify the original national data/document (i.e. that in use in their national infrastructure) this epSOS record comes from.

3.1.2.2 e1-REQ-2090 Recording of transcoded/translation data

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

Related to e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Each coded concept used to described the information identified by the epSOS functional specifications – where applicable - must be subject of a transcoding/translation process within the NCP.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.1.3 e1-FLD-71 Implementable Perspective

3.1.3.1 e1-REQ-2074 CDA conformance

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

The epSOS documents must be CDA conformant as per section 1.3 of the CDA Release 2.0 Normative Web Edition, May, 2005.

The originator and the recipient must fulfill their responsibilities as indicated in the section 1.3.1 Recipient Responsibilities and section 1.3.2 Originator Responsibilities from the respective document. Additional recipient requirements are described in specifications.

3.1.3.2 e1-REQ-2075 epSOS CDA Recipient Responsibilities

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

Document recipient shall be able – beside the baseline requirements of the 1.3.1 paragraph of the CDA R2 standard - to parse, interpret and if applicable display - all the coded entries (including related <translation> elements) labeled as “required” by the specification document D3.9.1 Appendix B1.

For **safety reasons** Care Providers accessing the epSOS CDAs should be enabled to visualize:

either the CDA level 3, either the CDA Level 1 format (i.e. the CDA with the PDF embedded), where applicable;

for each coded element required by D3.9.1 Appendix B1 specification, both the original country A representation and the epSOS representation. (either with the country B designation and with the epSOS (English) designation).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.1.3.3 e1-REQ-2076 Coded elements attributes optionality

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

In order to allow the transcoding/translation of the coded concepts pointed out by the epSOS functional specifications (WP 3.1 and 3.2), all these elements SHALL have (if applicable) the codeSystem attribute valorized.

3.1.3.4 e1-REQ-2077 Valorization of displayName

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

The official concept code designations – used for valorizing the attribute displayName – are defined by the Master Valueset Catalogue.

These values may be subject to changes: implementers should always refer to the latest published version of the MVC. Designations are reported in D3.9.1 Appendix B1 specification - if not otherwise specified - only for exemplification purposes.

3.1.3.5 e1-REQ-2078 Link between coded elements and text

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

It's strongly recommended for coded elements to valorize also the related originalText.reference element, in order to underline the link between the coded entries and the Section narrative part.

3.1.3.6 e1-REQ-2079 Document Instance Identifier

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

A CDA instance is uniquely identified by its ClinicalDocument.id.

A transformed document represents a new instance of the original document: transforming and

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

transformed CDA shall therefore have different ClinicalDocument.id values. The relationship between these two instances must be kept via the relatedDocument association.

3.1.3.7 e1-REQ-3894 Links among documents

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

Depending on the document type, every instance of epSOS pivot CDA shall have a related CDA embedding the PDF representation of the original data from which the epSOS pivot has been derived (also known as “epSOS PDF”).

3.1.3.8 e1-REQ-2080 Consumer capabilities (epSOS PDF)

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

The end user shall be able to access the epSOS PDF – if existing - any time it deems it is necessary for the document content comprehension.

3.1.3.9 e1-REQ-2081 Implementable Original document identification

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Implemented by e1-REQ-3900 Original document identification

Related to e1-REQ-2094 Patient Summary template conformance

Implemented by e1-REQ-1988 Peering Original Document

The relationship between the eP/eD/PS instance and the record (document) in use in the National Infrastructure (“original Country-A document”) must be kept via the XFRM relationship [XFRM (transform) = “The current document is a transformation of the ParentDocument”]. This relationship is mandatory.

The “national” document must be uniquely identified with its ID in context of the relatedDocument/parentDocument association (“aa-bb-cc” in the example).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.1.3.9.1 e1-TXT-283 Example

```
<relatedDocument typeCode="XFRM" >
  <parentDocument>
    <id root="aa-bb-cc" />
  </parentDocument>
</relatedDocument>
```

Even for countries not dealing with real documents in their National Infrastructures (e.g. data collected from local databases), this mechanism could be useful to identify the collection of data used for generating the epSOS CDAs , facilitating the information backtracking. In that case the ID might be that of the epSOS friendly document or of any other kind of intermediate document used for generating the NCP document input.

3.1.3.10 e1-REQ-2082 epSOS PDF – epSOS pivot link

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

The link between the epSOS pivot and the epSOS PDF **may** be derived at the document level in three ways:

both have the same relatedDocument(XFRM).parentDocument

if used, both have the same setId. This value should be equal to the “national document” setId, if existing.

the pivot have a relatedDocument relationship with the epSOS PDF.

This relationship should be represented as follows

```
<relatedDocument typeCode="APDN" >
  <parentDocument>
    <id root="aa1-bb1-cc1" />
  </parentDocument>
</relatedDocument>
```

Where aa1-bb1-cc1 is in this example the ID of the epSOS PDF.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.1.3.10.1 e1-TXT-447 Note

Even if no one of the allowable relationship defined by the CDA standard (XFRM, RPLC, APDN) fits perfectly with the relationship existing between the pivot and the PDF CDA; the APND relationship seems to be that better describing the epSOS scenario. In fact “An addendum is a separate document that references the parent document, and may extend or alter the observations in the prior document. The parent document remains a current component of the patient record, and the addendum and its parent are both read by report recipients.”

Example: This relationship would be therefore represented as follows:

```
<relatedDocument typeCode="APND" >
  <parentDocument>
    <id root="aa1-bb1-cc1" />
  </parentDocument>
</relatedDocument>
```

Where aa1-bb1-cc1 is in this example the ID of the epSOS PDF.

3.1.3.11 e1-REQ-2091 Element <translation>

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

Related to e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-3895 Element <translation> - Transcoding in country A

Related to e1-REQ-3896 Element <translation> - Translation in country B

As a result of transformation (transcoding / translation), for each coded element successfully processed, a nested <translation> elements shall be added.

It shall also keep English translation of epSOS coded concept.

Translation element may contain the same set of information as the original coded element, i.e. code, codeSystem (OID), codeSystemName, displayName.

At the same time, the original code and English version of epSOS code shall be kept, enabling the receiver to look it up if needed.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.1.3.11.1 e1-TXT-448 Example

```
<translation
code="230291001"
codeSystem="2.16.840.1.113883.6.96"
codeSystemName="SNOMED CT"
displayName="Juvenile Parkinson's disease"/>
```

3.1.3.11.2 e1-REQ-3895 Element <translation> - Transcoding in country A

Related to e1-REQ-2091 Element <translation>

As a result of transcoding in country A, translation element must be nested into original coded element (first nested level inside original coded element).

3.1.3.11.3 e1-TXT-449 Example

```
<value xsi:type="CE" code="G20"
codeSystem="1.3.6.1.4.1.12559.11.10.1.3.1.44.2"
codeSystemName="ICD10"
displayName="Parkinson's disease">
<translation
code="230291001"
codeSystem="2.16.840.1.113883.6.96"
codeSystemName="SNOMED CT"
displayName="juvenilná Parkinsonova choroba"/>
</value>
```

3.1.3.11.4 e1-REQ-3896 Element <translation> - Translation in country B

Related to e1-REQ-2091 Element <translation>

As a result of translation in country B, another translation element shall be created and nested below original coded element (first nested level inside original coded element). Already existing translation element created by transcoding in country A, shall be shifted one level below and nested to the new translation element (second nested level inside original coded element).

If some of the data is the same as in the element having nested translation element, these should not be repeated again.

If original coded element contains other nested elements, these shall be kept without any change in transformed document.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.1.3.11.5 e1-TXT-450 Example

Result of translation in country B:

```
<value xsi:type="CE"
  code="G20"
  codeSystem="1.3.6.1.4.1.12559.11.10.1.3.1.44.2"
  codeSystemName="ICD10"
  displayName="Primäres Parkinson-Syndrom">
  <translation
    displayName="Parkinson's disease">
    <translation
      code="230291001"
      codeSystem="2.16.840.1.113883.6.96"
      codeSystemName="SNOMED CT"
      displayName="juvenile Parkinson's disease"/>
  </translation>
</value>
```

code, codeSystem and codeSystemName of <value> Element are the same as in its child element <translation>:

```
<value xsi:type="CE"
  code="230291001"
  codeSystem="2.16.840.1.113883.6.96"
  codeSystemName="SNOMED CT"
  displayName="Juvenile Parkinson's disease">
  <translation
    displayName="juvenile Parkinson's disease"/>
</value>
```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.1.3.12 e1-REQ-2092 Reference coded system used in Country A

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

Related to e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

There is a special case, when Country A uses the same code system as epSOS chosen for reference system. In that case, transcoding to another code system in country A shall not be done. Transformation shall just add English display name in such case.

As a result of transformation in country B, new <translation> element shall be added to coded element. Data obtained from terminology repository as transcoding of coded concept shall replace original data of the element and the original data shall be stored in another <translation> element. Already existing <translation> shall be nested into the new one.

3.1.3.12.1 e1-TXT-285 Example

Then, format of resulting CDA element could look like:

```
<value xsi:type='CE'
      code="43116000"
      codeSystem="2.16.840.1.113883.6.96"
      codeSystemName="SNOMED CT"
      codeSystemVersion="July2009"

      displayName="Ekzem">

    <translation displayName="Eczema">
      <translation displayName="vyrážka"/>
    </translation>
</value>
```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.1.3.13 e1-REQ-2097 epSOS pdf conformance

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance

Related to e1-REQ-2094 Patient Summary template conformance

The epSOS pdf SHALL conform this rules:

The encoding rules of the pdf, including the allowed pdf formats, SHALL be the same defined by the IHE XDS-SD profile

The epSOS PDF document code SHALL be one of those defined in D3.9.1 Appendix B1 Chapter 4 "LOINC codes" and SHALL be the same used for the related epSOS pivot

The epSOS PDF and the epSOS pivot SHALL use the same patient ID

The epSOS PDF SHALL refer the same "Original document" of the epSOS pivot as defined in D3.9.1 Appendix B1 11.1.2.1 "Original document identification"

The epSOS PDF SHOULD apply the same optionality and cardinality rules of the header elements defined in D3.9.1 Appendix B1 Chapter 10.1 "Header Data Elements" for the epSOS pivot.

3.2 e1-FLD-68 Patient Identification

3.2.1 e1-FLD-72 Conceptual Perspective

3.2.1.1 e1-FLD-151 Information Dimension

3.2.1.1.1 e1-REQ-1668 About Patient Identification in the ePrescription

Synchronized with e1-REQ-5138 About Patient Identification in the ePrescription

Synchronized with e1-REQ-5139 About Patient Identification in the ePrescription

Synchronized with e1-REQ-5140 About Patient Identification in the ePrescription

Synchronized with e1-REQ-5141 About Patient Identification in the ePrescription

Related to e1-REQ-5135 Minimum data elements for searching a patient

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Variable	Definitions	MS: Minimum Optional	Comments	Example
Given Name	The Name of the patient	Yes	This field can contain more than one element	Marta
Family Name/Surname	The surname/s of the patient	Yes	This field can contain more than one element	Español Smith
Gender	The gender of the patient	Yes		Male/female/unknown
Birth date	Date of birth	Yes	This field may contain only the year	01/01/2009
Regional/National Health Id	If the patient has a regional or national Health Identification	Yes	This field is required by some national laws	
Social/Insurance Number		Yes	If a patient has both, national/regional ID and Social/Insurance number, only the regional/national Health Id is required by law. If the only identification the patient has is the Social/insurance number, then this one is considered as the regional/national Health Id. This field is required by some national laws.	

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.2.1.1.2 e1-REQ-5135 Minimum data elements for searching a patient

Related to e1-REQ-1668 About Patient Identification in the ePrescription

- Surname
- Given Name
- Date of birth (YYYYMMDD)
- Gender
- Country of origin
- Unique Identifier (if available)
- Other identifiers (e.g.: ID number, driving license number, passport number, etc.)

Additional data elements, if necessary in different MS, can be added (e.g. address)

3.2.1.2 e1-FLD-150 Computational Dimension

3.2.1.2.1 e1-REQ-4412 Process Identification & authentication of a patient with demographic data

Related to e1-REQ-1973 Patient Identification

Related to e1-REQ-4603 REQ 3.3.18 Patient Identification accomplished by HP-B

Related to e1-REQ-4418 REQ 3.6.2 National identity registers

Related to e1-REQ-4415 REQ 3.6.23 Patient's authentication with demographic data

Related to e1-REQ-4416 REQ 3.6.24 Patient's authentication with extended demographic data

Related to e1-REQ-4413 REQ 3.6.4 Wildcards in demographic queries

Related to e1-REQ-4414 REQ 3.6.5 Handle "more than one" demographic matches

Related to e1-REQ-1951 Traits Handshake central function

Related to e1-REQ-4846 Unique Patient Identifier

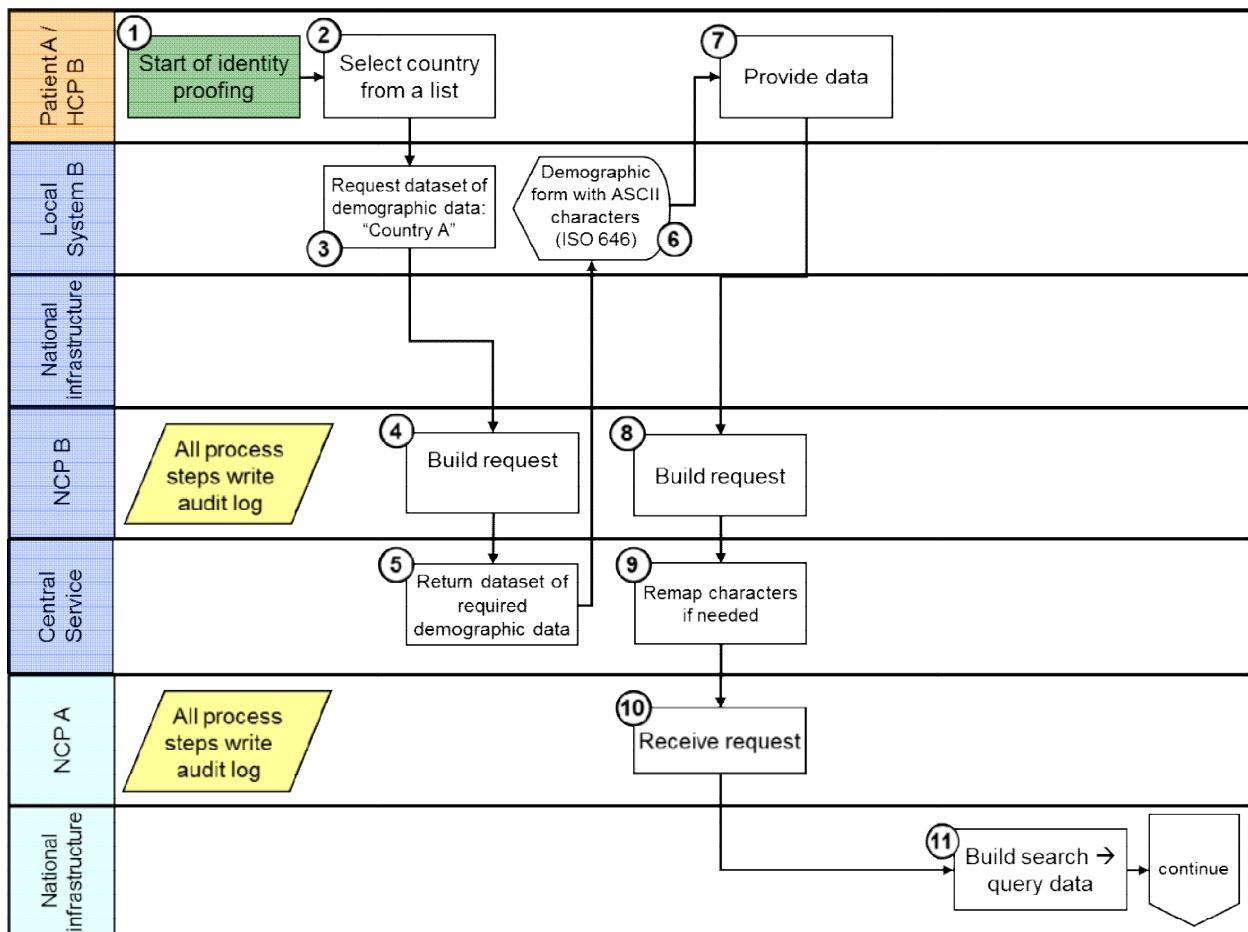
Related to e1-REQ-4634 epSOS IdentificationService Service Interface & Functional Specification

Related to e1-REQ-4635 Patient Identification Components Communication Workflow

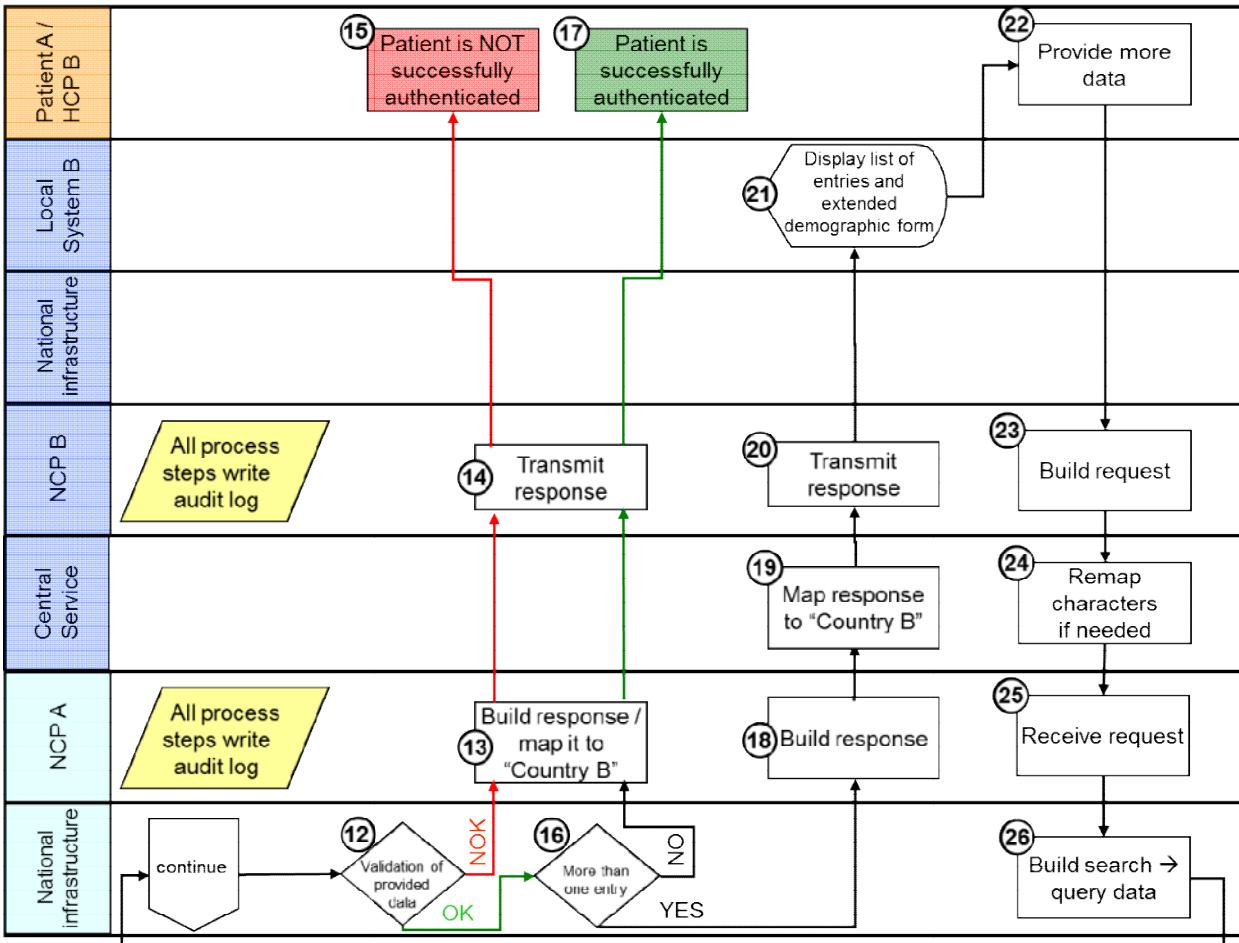
Patient of "Country A" at a "Point of Care (PoC)" in "Country B" and has no "eID"

This process describes the case of a patient of Country A, who wants to be identified and authenticated for epSOS LSP in Country B at the PoC without having an eID. The patient needs some trustworthy document with photo and with demographic data. Demographic data itself is stored in national infrastructure in Country A (national registry in Country A) (for details, see pictures and descriptions below).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013



	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



The process depicted consists of the next steps:

1. The patient is situated in CountryB at the PoC and wants to be identified and authenticated. As a precondition, the patient has to show a trustworthy document (e.g. driving license, passport) as an identifier to the HP. This is the starting point of the identification and authentication process. The first step in this process includes the revalidation of the authorization of the HP for epSOS LSP.
2. The patient tells the HP the name of "his country of affiliation" (Country A) and based on this information, the HP makes the selection of the appropriate country from a list, provided by the local system.
3. Then the local system (at PoC) requests from the NCP B the required dataset of demographic data for Country A.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

4. NCP B receives the request from the local system and writes a record into audit log. Then the NCP B builds the request and sends it to the Central Services layer.

Note: The definition of needed dataset may vary from country to country and may change over the time. E.g. France needs only a predefined ID (instead of concrete demographic data) which identifies French citizens and Germany has some special requirements as part of the usage of pseudonyms and TANs for data privacy reasons based on the German legislation. Any changes of these datasets should be maintained by the concerned country itself and stored in the Central Services layer.

5. Then the appropriate part of the Central Services returns the required dataset of demographic data for Country A to the local system at PoC and writes this event into audit log.

Note: Of course this is not done in a direct way (Central Services send back the information to NCP B and NCP B sends the information to the local system) these is just drawn in a short way to make the picture easier to read.

6. The local system displays the form to enter the appropriate demographic data (e.g. for French patients just one field to enter the ID or for German patients the required fields to enter a pseudonym and a TAN). If used the fields for "Surname" and "Given name" must be appropriately adapted in length and format (e.g. name prefix for ES and NL). This form uses ASCII characters (as defined by ISO 646) for entering demographic data to avoid misspelling errors raised by "foreign" characters. The permission of how to use "wildcards" (replacing characters by a single character e.g. "?", "*") must be defined by each MS.

7. Patient provides the appropriate demographic data to the HP, who enters them into the local system at PoC, exactly as written in the patient's document or printed on an identification card. The patient's demographic data is sent to NCP B.

8. The NCP B receives data from local system and writes this event into audit log. Then the NCP B builds the request and hands it over to Central Services. Central Services map it into the predefined format for Country A. The request for patient authentication is transmitted to NCP A and the transmission is recorded into audit log.

9. Central Services map it into the predefined format for Country A. The request for patient authentication is transmitted to NCP A and the transmission is recorded into audit log.

10. NCP A receives the request from NCP B and remaps characters (if needed). NCP A writes a record into audit log. NCP A sends the received identification and authentication data to the national infrastructure and writes a record into audit log.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

11. The national infrastructure takes the identification and authentication data and builds a request for search. Number of returned data records of this query is limited.

Note: The limitation of returned data is an assumption and has to be defined by Country A. If there are more matches than this limit, the "quality" or the number of entered identification and authentication data can be seen as inaccurate and more data values are necessary to decrease the number of possible matches.

12. The national infrastructure performs a search (trying to validate identification and authentication data – credentials) against stored data in a national registry.

One of the following results is returned:

a. Validation of credentials is successful (at least one entry in the national registry conforms to the received demographic data) (continue with step 21) or

b. Validation of credentials is not successful (no entry in the national registry conforms to the received identification and authentication data) à patient is not authenticated.

13. NCP A receives an appropriate message from the national infrastructure and writes a record into audit log. Then NCP A builds the response, maps it into the predefined format for Country B and transmits the response to NCP B. NCP A writes this event into audit log.

14. NCP B receives the response from NCP A and writes a record into audit log. Then NCP B transmits the response to the system where HP wants to authenticate the patient and writes this event into audit log.

15. HP receives the message about failed authentication of the patient. The process is finished.

16. If just one entry in the national registry conforms to the received identification and authentication data of the patient, the patient is successfully authenticated and all unprotected demographic data will be returned to NCP A. Using the same algorithms as described in steps 13 and 14 the national infrastructure sends back the data to the HP in Country B.

If more than one entry in the national registry conforms to the received identification and authentication data, the patient is not yet successfully authenticated and more identification and authentication data values are required (the process continues with step 18).

17. HP confirms the authentication of the patient based on the returned demographic data and the process is finished.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

18. Country A decides what will be returned to Country B.

a. Option 1: The national infrastructure of Country A sends the list of matching entries to NCP A, limited by the national rules.

b. Option 2: No demographic data will be returned but a predefined value that Country B can derive that there are more matches than just one. This would support patient's privacy and prevent the HP from selecting the wrong patient record from the list of available matches.

Regardless of which option is used, the NCP A writes a record (NOT the data content!) into audit log. Then NCP A builds the response, maps it into the predefined format for Country B and transmits the response to NCP B. NCP A writes this event into audit log.

19. The Central Services layer of NCP B receives the response from NCP A, remaps or translates the response if needed and writes this event into audit log.

20. Then NCP B transmits the response to the local system of the HP at PoC.

21. The local system at PoC receives the response of Country A and displays the (probably extended) demographic form again.

22. Now the HP has 2 options:

a. If Country A sent back a list of matching entries (step 18, Option 1), he can select the specific record that matches the person which is standing in front of him based on additional identifiers (e.g. Passport) or

b. Enter more identification and authentication data of the patient and send the data to NCP B.

23. The NCP B receives data items from the local system of the HP. Then NCP B builds the request again and hands it over to Central Service.

24. Central Services map it into the predefined format for Country A and transmits the requests to the NCP A again. NCP A writes a record into audit log.

25. The NCP A receives the request from NCP B and writes an event into audit log. Then NCP A sends the identification and authentication data to the national infrastructure.

26. The national infrastructure takes over the identification and authentication data and processes the search algorithm again. Number of query data is still limited (as defined by Country A). Continue with step 12.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.2.1.2.2 e1-TXT-591 Messages that can occur within the patients processes

Related to e1-REQ-2265 Process Identification & authentication of a patient with demographic data

As already mentioned in the preconditions of the above described processes the patient must be registered in a national directory which is a part of the national infrastructure of Country A. Regarding the single process steps the following (error) messages could show up:

- “No information about Country A is available neither in Country B nor in epSOS.”
- “Connection to Country A failed. Identification, authentication and authorisation of a patient is not available.”
- “The expected Level of trust of patient’s identification, authentication and authorisation in Country A is higher than the offered one.”
- “The expected Level of trust of the HCP is higher than the offered one.”
- “The offered eID or identification and authentication data of the patient could not be found in Country A.”
- “The offered identification and authentication data return more matches than allowed in Country A.”

3.2.2 e1-FLD-73 Logical Perspective

3.2.2.1 e1-REQ-4603 REQ 3.3.18 Patient Identification accomplished by HP-B

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

Patient shall present to health profesional at PoC-B some accepted identification means which are accepted by national policy of country A. If necessary a health specific ID may be given to health profesional at PoC-B in accordance with the requirements of NCP-A. NCP-B shall query NCP-A with entered data; The ID query MAY come up with a new identifier provided by NCP-A.

3.2.2.2 e1-REQ-4418 REQ 3.6.2 National identity registers

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

The national authorities must run identity registers and provide necessary information to authorised epSOS LSP actors.

3.2.2.2.1 e1-TXT-587 Note

epSOS LSP and authorities/participants from national domains will together provide identification and authentication services.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.2.2.3 e1-REQ-4413 REQ 3.6.4 Wildcards in demographic queries

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

Every PN should use the method of "Wildcards" in demographic queries whenever technical feasible to support the security issues and data privacy within epsOS LSP as good as possible.

3.2.2.4 e1-REQ-4414 REQ 3.6.5 Handle "more than one" demographic matches

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

The procedures of how to handle "more than one" matches in identification and authentication processes of patients must be defined by each PN.

3.2.2.5 e1-REQ-4415 REQ 3.6.23 Patient's authentication with demographic data

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

Any participating PN must establish organisational procedures and technical processes to allow the identification and authentication of its citizens by the usage of demographic data in an electronically format from abroad.

3.2.2.6 e1-REQ-4416 REQ 3.6.24 Patient's authentication with extended demographic data

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

If a PN needs more than the minimum data elements to search for a patient, the additional data elements must be stored on NCP A.

3.2.2.7 e1-REQ-4673 Patient Identification

Synchronized with e1-REQ-1973 Patient Identification

Related to e1-REQ-4846 Unique Patient Identifier

The intended recipient of medical data MUST identify the patient with sufficient accuracy. Medical data MUST only be disclosed after the patient was identified with sufficient accuracy.

Technical means for patient identification MUST NOT use or disclose medical data about this patient. Patient identifiers SHOULD NOT technically enable any unlawful linkage of the patient's medical data to other sanctioned personal data beyond any legitimate purpose from other domains. If technical means for identity protection (e.g. pseudonymization) are used, these

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

MUST NOT disqualify the responsible parties to lawfully provide the patient access to his/her data. The original identification of the patient MUST NOT rely on the existence of electronic identifiers (eIDs). epSOS use cases MAY define further constraints on the accuracy and means of patient identification for that specific use case (e.g. identification by name considered as insufficient for the 112 use case).

3.2.2.8 e1-REQ-4846 Unique Patient Identifier

Related to e1-REQ-1985 Patient Data Assignment

Related to e1-REQ-4673 Patient Identification

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

In order to discover a patient's medical data the patient must be identified and a unique patient identifier must be shared between the communicating NCPs.

This shared identifier MUST be used as a patient identifier as required by the epSOS medical data exchange services (e. g. *epSOS Patient Service* and *epSOS Order Service*). Nevertheless the country of the patient's affiliation is not restricted to provide an existing national patient ID as a shared identifier but MAY as well issue dedicated epSOS identifiers or use a patient pseudonym as the epSOS shared identifier

3.2.2.8.1 e1-TXT-735 Note

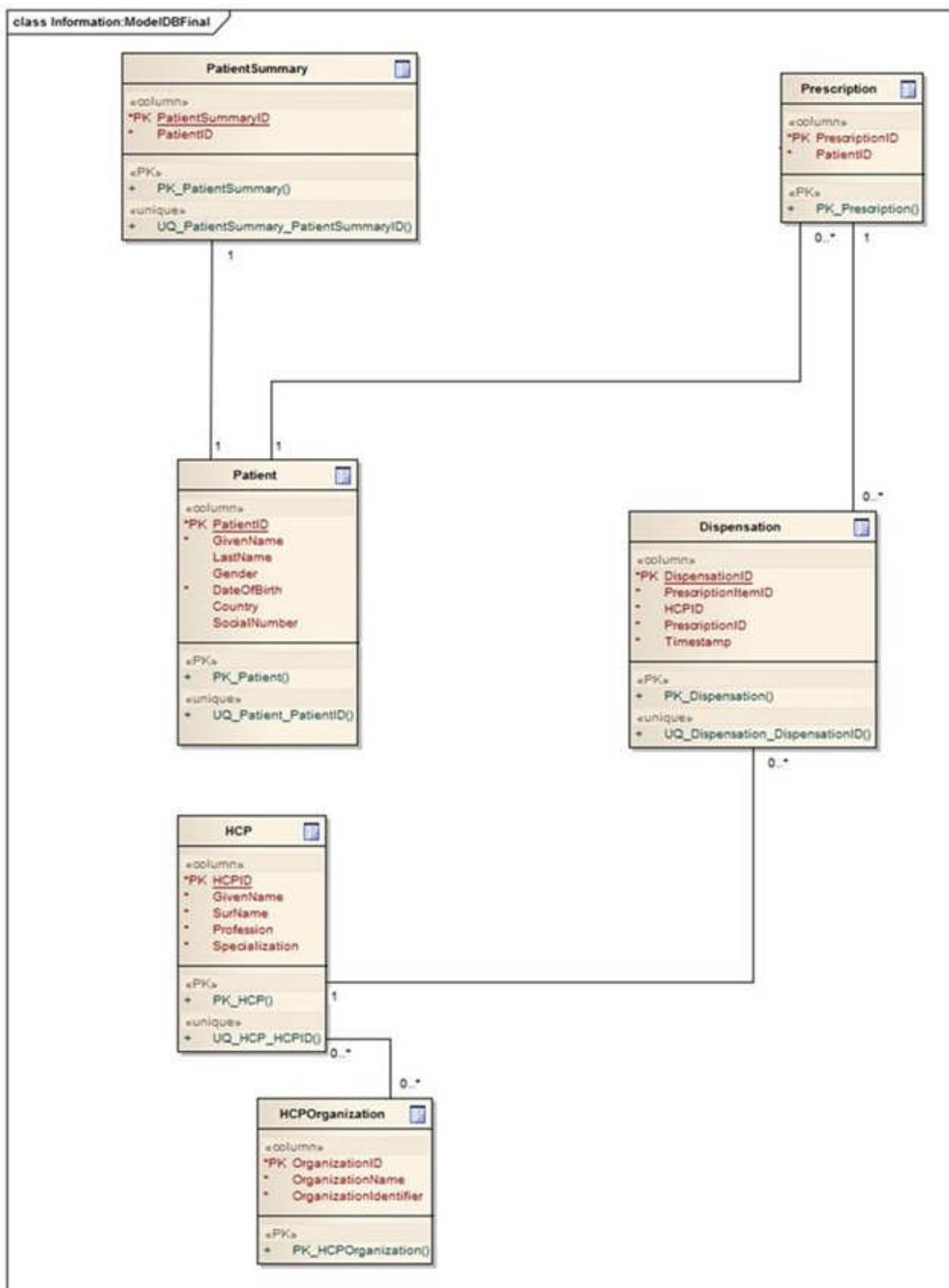
This shared identifier enables the medical data consuming services to properly reference that patient's data which is provided by the medical data providing services at the patient's country of affiliation.

The *epSOS Identification Service* defines means for the agreement on this shared identifier and for increasing the degree of accuracy of the patient identification that is performed at the point of care.

3.2.2.9 e1-FLD-143 Information Dimension

3.2.2.9.1 e1-REQ-4633 Information Model: Patient Summary & ePrescription

Synchronized with e1-REQ-4624 Information Model: Patient Summary & ePrescription



	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Health Professional (HP)

A health professional is a physician participating in epSOS identifiable by its unique id. It is affiliated to zero or more health care professional organizations, depending on national legislation.

The HP contains information as defined in D3.1.2. A HP is related to 0..n HCPOs and is associated with 1..n Healthcare Professional Addresses.

Health Care Professional Organization (HCPO)

A Health Care Professional Organization is a logical entity within the national environment known to the NCP and uniquely identifiable by its id.

The HCPO object contains information defined in D3.1.2. An HCPO is related to 1..n HPs. At any given time in the context of an epSOS transaction, an HP is associated with only one HCPO.

Patient

A patient is an individual person participating in epSOS by giving permission (prior consent) in his home community to process his/her medical data to a foreign participating nation.

The Patient object contains information defined in D3.1.2. A patient is related to 1..1 PS, 0..* ePs and 0..* eDispenses.

3.2.2.9.2 e1-TXT-728 Note

Identity is an abstract notion and usually the identity of an entity can be represented by an identifier. The identifier is a non-empty set of identity information that uniquely characterises an entity in a specific domain of applicability. Typical attributes which will be combined to identifiers, are the following personal data:

- Surname
- Given Name
- Date of birth (YYYYMMDD)
- Gender
- Country of origin
- Unique Identifier (if available)
- Other identifiers (e.g.: driver license number, passport no, etc.)

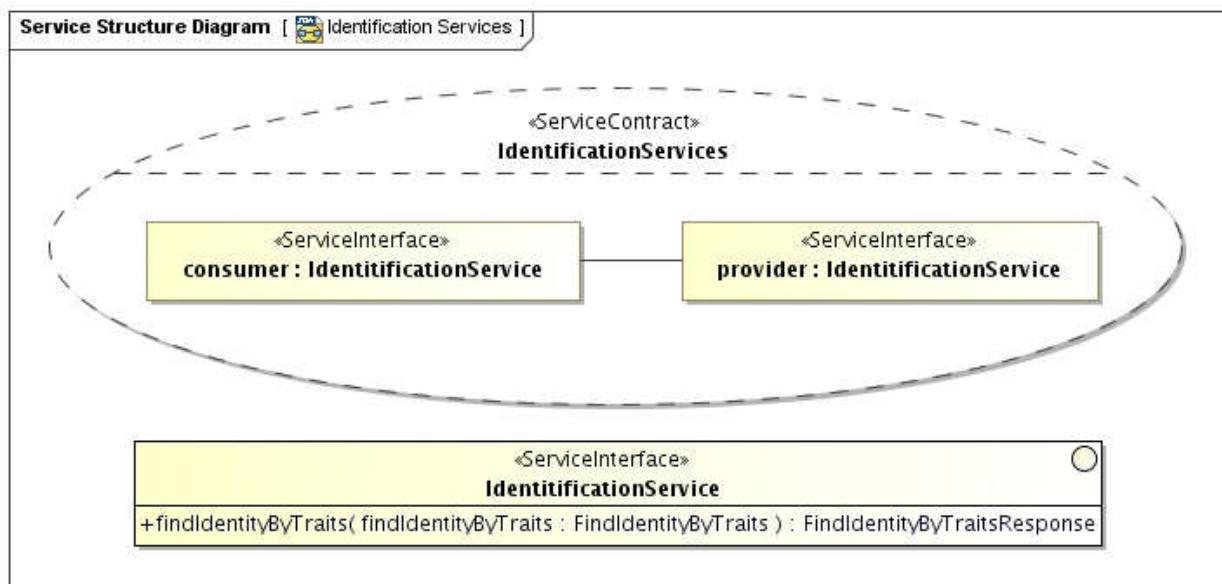
	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

3.2.2.10 e1-FLD-144 Computational Dimension

3.2.2.10.1 e1-REQ-4634 epSOS IdentificationService Service Interface & Functional Specification

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

Related to e1-REQ-4845 epSOS IdentificationService Service Interface & Functional Specification



Operation **findIdentityByTraits()**

Description Obtain a shared patient identifier by querying for patient identity traits

Requestor Consuming Gateway at NCP-B

Input Message **FindIdentityByTraitsRequest**

Body	(1) List of patient identity traits as provided by the patient to the HP. (2) optional: minimum confidence level that has to be met by the entities that match the provided traits.
------	--

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Security Token X.509 Gateway Certificate

epSOS HCP Identity Assertion

Output Message in successful Case	FindIdentityByTraitsResponse
Body	(1) Unique identifier of the patient that has to be used for all subsequent calls for this patient's medical data. (2) optional: further patient identity traits that allow the HP to verify the result of this operation.
Security Token	X.509 Gateway Certificate
Precondition of success scenario	The requestor is able to locate the service provider The certificate of the NCP-A gateway is available to the requestor. The requestor is able to verify the certificate of the NCP-A gateway. The NCP-A gateway is able to verify the requestor's certificate. An HCP identity assertion has been issued by NCP-B and is available to the requestor The NCP-A gateway is able to verify the validity of the HCP identity assertion
Main success scenario	Actions of the epSOS Patient Identification Service provider: validate the message signature and decrypt the message body verify HCP identity assertion extract the patient identity traits from the message body search for patients that match the provided ID attributes discard all patients from the candidates list who have not given consent to epSOS if no patient matches: throw respective fault

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

if multiple patients match: request for more identity traits

if single patient matches: select ID to be used for subsequent requests

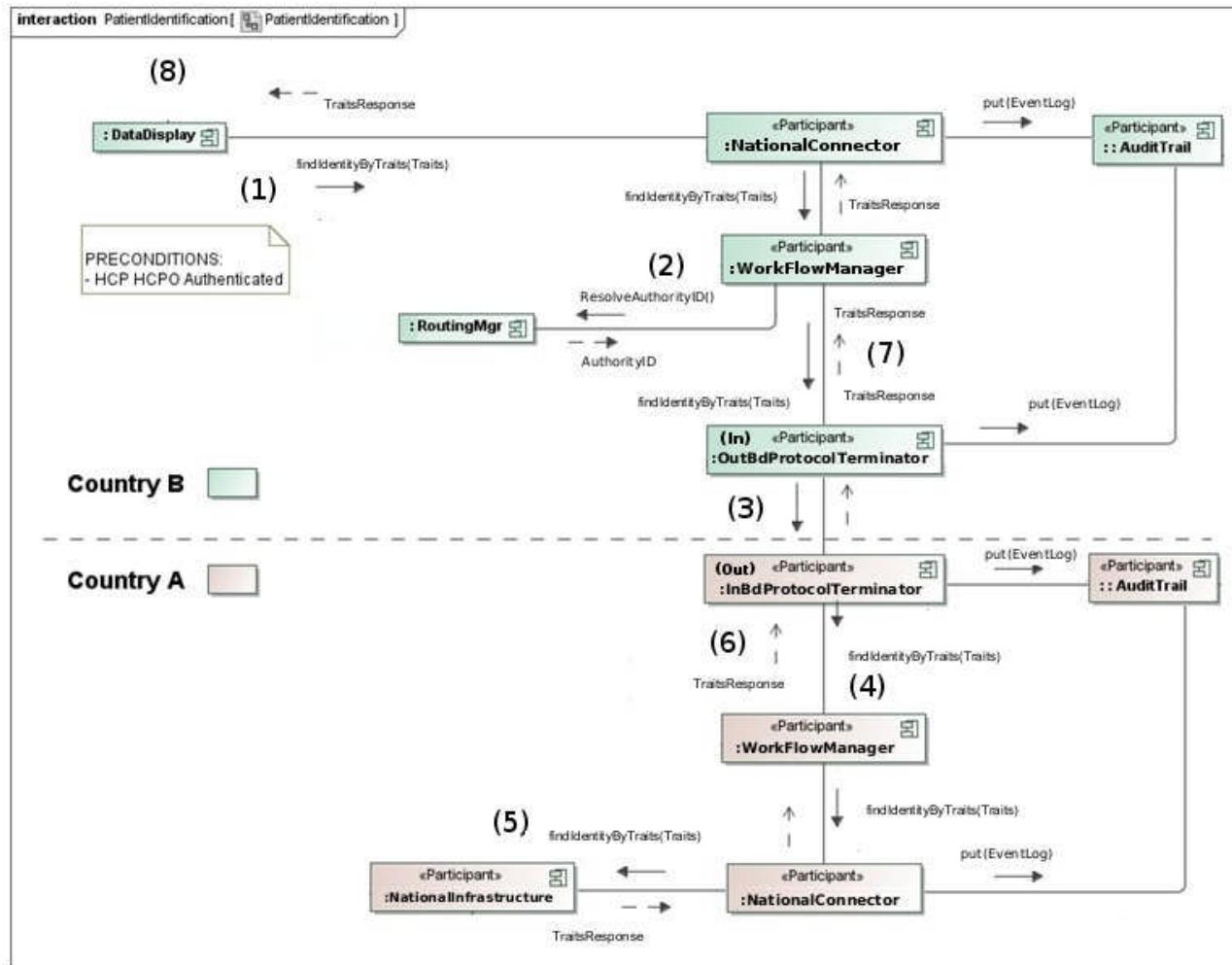
sign the response message and send it to the requestor

Fault Conditions	Preconditions for a success scenario are not given
	Requestor has insufficient rights to query for a patient's identity
	No matching patient is discovered that gave consent to epSOS
	ID traits are insufficient to find a unique match
	The confidence level of the matches is too low with respect to the level required by the requestor.

3.2.2.10.2 e1-REQ-4635 Patient Identification Components Communication Workflow

Related to e1-REQ-4412 Process Identification & authentication of a patient with demographic data

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version: 1.0
D5.2.3	Date: 31/01/2013



1. After the HP B is authenticated (precondition), the component dataDisplay initiates the searchPatient, by calling the right function located on the NationalConnector. The `findIdentityByTraits()` needs patient attributes as input arguments (The name of the transaction : `findIdentityByTraits()` is not mandatory, it is PN decision.) . All incoming transactions at the NationalConnector are audited by the AuditTrails component.
2. The request is forward to the WorkflowManager, where the business logic starts. The RoutingManager informs the WorkFlowManager for the NCP A destination.
3. The NCP B OutboundProtocolTerminator wraps the request into a SOAP envelope and sends it to the InboundProtocolTerminator at NCP A. Audit Trails at NCP B keeps track of what does leave from country B, as the same occurs in country A when the message arrives. Any incoming message that arrives to the InboundProtocolTerminator for the request contains the wrapped informations for the patient. Decoding and unwrapping is done inside in the

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

InboundProtocolTerminator.

4. The WorkflowManager extracts the identity traits from the object and uses them as an input arguments when calling NationalConnector for the findIdentityByTraits() operation.
5. The NationalConnector queries the patient Data result in from the national infrastructure in country A and then returns the object to the Workflow Manager. The transaction is audited by the AuditTrails component. The name of the transaction : findIdentityByTraits() is not mandatory, it is PN decision.
6. The Traits Patient Response goes back to NCP B through the same components (1-5), and arrives to the Inbound Terminator in B (previously named OutBoundTerminator when message goes out). Upon the arrival of the SOAP response, both ProtocolTerminator makes a corresponding record in the audit trail.
7. The WorkFlowManager at NCP B receives the unwrapped message from InboundProtocolTerminator and transmits the request to the NationalConnector in country B.
8. The Patient Identification Response Traits is returned to the originator of the request, the HP B.

3.2.2.10.3 e1-REQ-4839 MISSING PIN Workflow

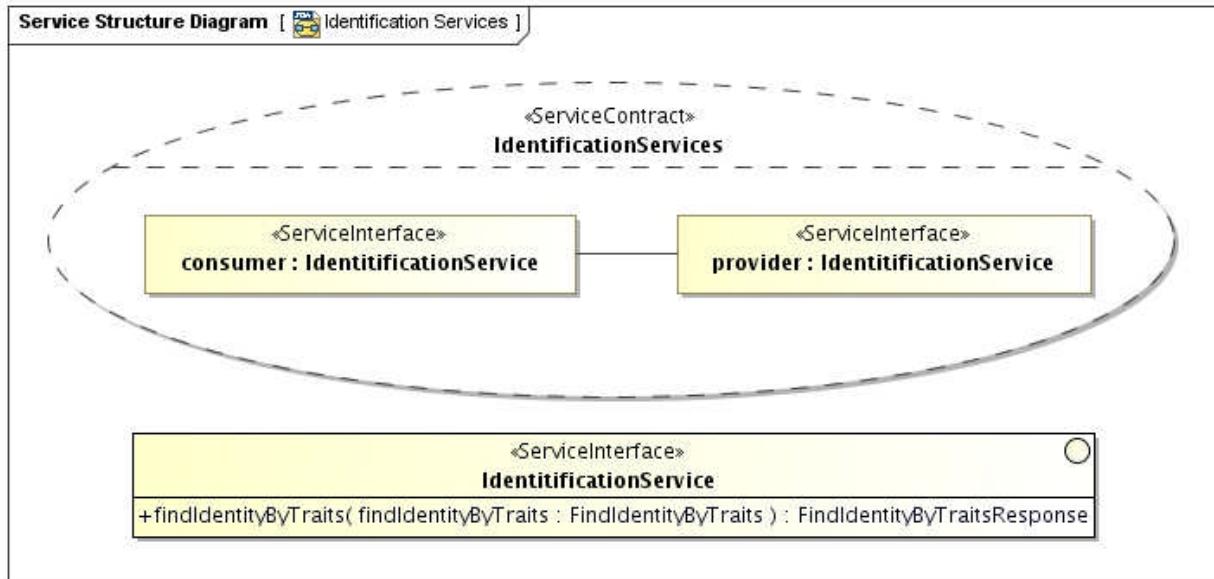
3.2.2.10.4 e1-REQ-4845 epSOS IdentificationService Service Interface & Functional Specification

Related to e1-REQ-4634 epSOS IdentificationService Service Interface & Functional Specification

Related to e1-REQ-4841 General Considerations for Successful Service Operations

Related to e1-REQ-4852 epSOS Identification Service Message Specification

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



Operation: `findIdentityByTraits`

Operation `findIdentityByTraits()`

Description Obtain a shared patient identifier

Requestor Consuming Gateway at NCP-B (service consumer at the country of care)

Input `FindIdentityByTraitsRequest`
Message

Body (1) List of patient identity traits as provided by the patient to the HP.
 (2) optional: minimum confidence level that has to be met by the entities that match the provided traits.

Security Token [1] [PT] X.509 NCP-B service certificate
 [ST] epSOS HCP Identity Assertion

Output `FindIdentityByTraitsResponse`

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Message in successful Case Body
(1) Unique identifier of the patient that has to be used for all subsequent calls for this patient's medical data.
(2) optional: further patient identity traits that allow the HP to verify the result of this operation.
If no unique match is found, the service provider MAY respond with a list of candidates. For each candidate body elements (1) and (2) MUST be provided.

Security Token	[PT] X.509 NCP-A service certificate
----------------	--------------------------------------

Precondition of success scenario In addition to the requirements stated in e1-REQ-4841 the following preconditions MUST be met for successful processing:
The patient has given a consent that authorises NCP-A to disclose his identity
The patient is able to provide identity traits that are sufficient for a unique identification

Main success scenario	Actions of the epSOS Identification Service provider: Validate the authenticity of the service consumer Verify HCP identity assertion Verify that the requesting HP is authorised to query for patient IDs Extract the patient identity traits from the message body Search for patients that match the provided ID attributes depending on the number of matches: If multiple patients match: request for more identity traits or provide a list of candidates (depending on national security policy). If a list of matching candidates is provided it MUST only include patients who gave consent to epSOS. If single patient matches and this patient has given consent to epSOS: select ID to be used for subsequent requests
-----------------------	--

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Any other case: throw respective fault

Apply epSOS protection means to the response message and send it to the requestor

Fault Conditions	Preconditions for a success scenario are not met
	Requesting HP has insufficient rights to query for a patient's identity
	No matching patient is discovered that gave consent to epSOS
	ID traits are insufficient for country A to find a matching patient (e.g. provided search criteria are not supported)
	The confidence level of the matches is too low with respect to the level required by the requestor
	Patient identification is only performed in conjunction with patient authentication (e.g. by providing a secret or a reference to a valid STORK authentication)
	Confirming the query would lead to a privacy violation acc. to country A legislation.

[1] PT = Protection Token, ST = Supporting Token (according to [WS SecurityPolicy] definition of security token types)

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.2.3 e1-FLD-159 Implementable Perspective

3.2.3.1 e1-FLD-160 Information Dimension

3.2.3.1.1 e1-REQ-4856 Use of Pseudonyms and Temporal Identifiers

A member state MAY wish to protect its patients' privacy by negotiating an epSOS shared identifier from a pseudonymous or temporal national patient identifier. In this case *Shared/national Patient Identifier Query and Feed mode* MUST be used. On successful identification within country A the response message MUST at least provide the patient's date of birth in order to allow the HP in country B to verify the accuracy of the identification.

3.2.3.1.2 e1-REQ-4854 Request Message

The *findEntityByTraits()* request MUST be initiated by an HP in the country of care for the identification of a foreign patient. The respective request message conforms to the *Patient Registry Find Candidates Query (PRPA_IN201305UV02)* interaction type as profiled by the IHE XCPD Cross-Gateway Patient Discovery transaction IHE XCPD August 2009.

For the HL7 transmission wrapper and the *HL7 Control Act* the conventions identified in the IHE PIX/PDQV3 August 2009 supplement appendix O and the changes from the XCPD August 2009 supplement appendix O MUST be followed.

In addition the following epSOS-specific restrictions apply:

MUST refer to NCP-A. Other sub-elements than the device-identifier that holds the OID of NCP-A MUST be ignored by the service provider and SHOULD NOT be provided by the service consumer. MUST refer to NCP-B. Other sub-elements than the device-identifier that holds the OID of NCP-B MUST be ignored by the service provider and SHOULD NOT be provided by the service consumer.

Asynchronous operations MUST NOT be used. According to D3.3.2 all message interchange in epSOS MUST be synchronous.

Demographic Query Only mode or Shared/national Patient Identifier Query and Feed mode MUST be used. Other modes defined in IHE XCPD August 2009 MUST NOT be used.

The *health data locator option* as defined in section 27.2.1 of IHE XCPD August 2009 MUST NOT be used. Where indication of support for the *health data locator option* is required in responses, the service provider MUST provide the value "NotHealthDataLocator".

The *revoke option* as defined in section 27.2.2 of IHE XCPD August 2009 MUST NOT be used.

Correlations MUST NOT be cached by the service provider. The respective syntax elements described in section 3.55.4.1.2 of IHE XCPD August 2009 MUST NOT be used.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Reverse Cross-Gateway Queries MUST NOT be used. The *homeCommunityId* and *community patient id assigning authority* arguments SHOULD be set to the OID of the responding NCP (NCP-A) in query requests.

3.2.3.1.3 e1-REQ-4869 Response Message (Full Success Scenario)

Related to e1-REQ-4859 Expected Actions

The epSOS findEntityByTraits response content MUST be based on HL7 Patient Registry Find Candidates Query Response (PRPA_IN201306UV02) interaction, as profiled by the IHE XCPD Cross-Gateway Patient Discovery August 2009 result message.

For the HL7 transmission wrapper and the HL7 Control Act the conventions identified in the IHE PIX/PDQV3 supplement appendix O and the changes from the XCPD supplement appendix O MUST be followed.

In addition the following epSOS-specific restrictions apply:

MUST refer to NCP-B. Other sub-elements than the device-identifier that holds the OID of NCP-B MUST be ignored by the service consumer and SHOULD NOT be provided by the service provider. MUST refer to NCP-A. Other sub-elements than the device-identifier that holds the OID of NCP-A MUST be ignored by the service consumer and SHOULD NOT be provided by the service provider.

Asynchronous operations MUST NOT be used. According to D3.3.2 all message interchange in epSOS MUST be synchronous.

Correlations MUST NOT be cached by the service provider. The respective syntax elements described in section 3.55.4.1.2 of IHE XCPD August 2009 MUST NOT be used.

The MUST be set to “D” (debugging) for epSOS pilot phase 1. It MUST be set to “P” (production) for epSOS pilot phase 2 and regular operations.

For each matching candidate a single element MUST be included within the control act wrapper. In addition to the constraints defined in IHE XCPD August 2009 the following conventions MUST be followed for elements:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Element Name	Opt.	epSOS Usage Convention
Patient	R	For each matching candidate a single element MUST be provided.
Patient/id	R	This element MUST contain the HL7-II-encoded Id of the patient that MUST be used for subsequent transactions to access the patient's medical data. The root designator MUST be present.
Patient/statusCode	R	MUST be "active".
Patient/patientPerson	R	Additional demographic data on a patient that matches the query. The encoding of this data MUST follow the conventions as stated in IHE XCPD August 2009. See table below for a list of demographics that SHOULD be used for epSOS.
Patient/subjectOf1/queryMatchObservation	R	This element encodes the score of the match as an HL7 observation. It MUST be used as this:

Other elements MAY be provided within the result set by the sender but SHOULD be ignored by the receiver.

For a *FindIdentityByTraits* response only the following ID data MUST be provided as child elements of the element.

Identity Data	Opt.	Usage Convention (if provided)
asOtherIDs/id	O	This element SHOULD be only given if it provides further information on the scope and context of the used identification mechanism. This information SHOULD be suited to allow the HP to verify the claimed identity of the patient.
Name	O	Both family name and given name SHOULD be provided. Note: This element is mandatory wrt. the HL7v3 schema. Therefore at least an empty instance MUST be included

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

		with the response.
birthTime	R+	MUST be provided as “YYYY[MM[DD[HHMM[SS[.S[S[S[S]]]]]]][+/-ZZZZ]”
birthplace	O	SHOULD contain the country and city of birth
administrativeGenderCode	O	
Addr	O	Only city and streetName SHOULD be provided
Guardian	X	For the 2011 epSOS pilots minors and dependent people will not be treated different from others. This element MUST NOT be provided as no respective risk assessment has been done.

As specified in IHE XCPD August 2009, the following status should be returned:

AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper).

OK (data found, no errors) is returned in QueryAck.queryResponseCode (control act wrapper)

3.2.3.1.4 e1-REQ-4870 epSOS Identification Service Errors and Warnings

Related to e1-REQ-4859 Expected Actions

If the *epSOS Identification Service* provider does not find a matching patient identifier it SHOULD include a <reasonOf/> element with the response message:

```
<reasonOf typeCode="RSON">
  <detectedIssueEvent classCode="ALRT" moodCode="EVN">
    <code code="ActAdministrativeDetectedIssueCode" codeSystem="2.16.840.1.113883.5.4"/>
    <!-- details on detected issue and proposed activity -->
  </detectedIssueEvent>
</reasonOf>
```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Depending on the reason for not providing a patient identifier, the codes and messages as defined below MUST be used [1]:

Condition and proposed action	Reason Encoding
<p>The service requestor tried an identification based on an ID only or did not provide enough data to univocally identify the patient. (WARNING)</p> <p>The HP SHOULD ask the patient for further demographics and re-issue the request.</p> <p>AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper).</p> <p>OK (data found, no errors) is returned in QueryAck.queryResponseCode (control act wrapper)</p>	<pre><triggerFor typeCode="TRIG"> <actOrderRequired classCode="ACT" moodCode="ENV"> <code code="AdditionalDemographicsRequested" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </actOrderRequired> </triggerFor></pre> <p>If specific demographics are requested the respective code values of code system 1.3.6.1.4.1.19376.1.2.27.1 as specified in section 3.55.4.2.2.6 of IHE XCPD SHOULD be used. There may be as many triggerFor elements, each of them containing an ActOrderRequired element as needed to code the attributes which would increase the assurance of the match [2].</p>
<p>The service provider only allows for patient identification by national/shared ID (WARNING).</p> <p>The HP SHOULD ask the patient for a national (health care) identification card and re-issue the request using <i>Shared/national Patient Identifier Query and Feed mode</i>.</p> <p>AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper).</p> <p>AE (application error) is returned in QueryAck.queryResponseCode (control act wrapper)</p>	<pre><triggerFor typeCode="TRIG"> <actOrderRequired classCode="ACT" moodCode="ENV"> <code code="DemographicsQueryNotAllowed" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </actOrderRequired> </triggerFor></pre>
The service provider only allows for patient identification by national health card or EHIC. Queries based on demographics only are not	<pre><triggerFor typeCode="TRIG"> <actOrderRequired classCode="ACT" moodCode="ENV"> <code code="EHICDataRequested"</pre>

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

<p>supported (WARNING)</p> <p>The HP SHOULD ask the patient for a health care identification card and re-issue the request.</p> <p>AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper).</p> <p>AE (application error) is returned in QueryAck.queryResponseCode (control act wrapper)</p>	<pre>codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </actOrderRequired> </triggerFor></pre>
<p>The service provider does not accept the query because responding MAY lead to a disclosure of private patient data (ERROR).</p> <p>The HP SHOULD limit the provided traits and re-issue the request.</p> <p>AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper).</p> <p>AE (application error) is returned in QueryAck.queryResponseCode (control act wrapper)</p>	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="PrivacyViolation"> codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy></pre>
<p>The requestor has insufficient rights to query for patient's identity data (ERROR).</p> <p>If access to the patient's medical data is required at the PoC this MUST be performed by a person with additional permissions.</p> <p>AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper).</p> <p>AE (application error) is returned in QueryAck.queryResponseCode (control act wrapper)</p>	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InsufficientRights"> codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy></pre>
Patient authentication MUST be piggybacked with patient identification. A respective identifier	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"></pre>

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

(e.g. GSS TAN) was not provided (ERROR) The HP at the PoC SHOULD ask the patient for a respective identifier and SHOULD re-issue the request. AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper). AE (application error) is returned in QueryAck.queryResponseCode (control act wrapper)	<code code="PatientAuthenticationRequired" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy>
The service provider did not find a match with the given minimum accuracy. (INFO) The service consumer SHOULD re-issue the request with a lower minimum confidence level. AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper). OK (data found) is returned in QueryAck.queryResponseCode (control act wrapper)	<mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy>
The identity traits provided by the service consumer are not supported by the service provider. (ERROR) The service consumer SHOULD re-issue the request with a different set of identity traits. AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper). AE (application error) is returned in QueryAck.queryResponseCode (control act wrapper)	<mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy>
The service consumer defined a confidence level that conflicts with the security policy of the service provider. (INFO)	<mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="PolicyViolation"

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The service provider SHOULD respond only with the candidate matches that it is allowed to provide wrt. its security policy. AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper). AE (application error) is returned in QueryAck.queryResponseCode (control act wrapper)	codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy>
--	--

[1] All codes using the coding system: codeSystem="1.3.6.1.4.1.19376.1.2.27.3 are to be used per XCPD error code definition.

[2] See IHI ITI CP #535

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.2.3.1.5 e1-REQ-4871 epSOS Identification Service Security Audit Considerations

Related to e1-REQ-1840 epSOS Patient ID Mapping Audit Schema

Both the epSOS *Identification Service* provider and consumer write an audit trail entry according to the ID Mapping audit schema as defined in e1-REQ-1840.

The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event
Human Requestor	R	HP who triggered the event
Source Gateway	R	Service consumer node address at the country of care
Target Gateway	R	Service provider node address at the country of affiliation
Mapping Service	R / X	Service that provided the mapping. MUST be filled by the service provider. MUST NOT be filled by the service consumer.
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient Source	R	Patient whose identifier was discovered or mapped
Patient Target	R	Result of the mapping operation
Error Message	O	Only used in case that the transaction was not completed successfully

3.2.3.1.6 e1-TXT-739 Example Request Message

The following excerpt from a *findEntityByTraits* request message shows the IHE XCPD profile of the HL7 PRPA_IN201305UV02 interaction type. The request message can be used to retrieve the identifier of a patient who identified himself with his electronic health card and date of birth.

```
<soapenv:Envelope>
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
<hl7v3:PRPA_IN201305UV02 xmlns:xsi="...">
```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<hl7v3:id root="36E66A20-1DD2-11B2-90FA-80CE4046A4A7"/>
<hl7v3:creationTime value="20100304120000"/>
<hl7v3:interactionId root="2.16.840.1.113883.1.6" extension="PRPA_IN201305UV02"/>
<hl7v3:processingCode code="P"/>
<hl7v3:processingModeCode code="T"/>
<hl7v3:acceptAckCode code="NE"/>

<hl7v3:receiver typeCode="RCV">
  <hl7v3:device classCode="DEV" determinerCode="INSTANCE">
    <hl7v3:id root="1.2.840.114350.1.13.999.234"/>
  </hl7v3:device>
</hl7v3:receiver>

<hl7v3:sender typeCode="SND">
  <hl7v3:device classCode="DEV" determinerCode="INSTANCE">
    <hl7v3:id root="1.2.840.114350.1.13.999.567"/>
  </hl7v3:device>
</hl7v3:sender>

<hl7v3:controlActProcess classCode="CACT" moodCode="EVN">
  <hl7v3:code code="PRPA_TE201305UV02" codeSystem="2.16.840.1.113883.1.6"/>

  <hl7v3:queryByParameter>
    <hl7v3:queryId root="1.2.840.114350.1.13.28.1.18.5.999" extension="18204"/>
    <hl7v3:statusCode code="new"/>
    <hl7v3:responseModalityCode code="R" />
    <hl7v3:responsePriorityCode code="I"/>

    <hl7v3:parameterList>
      <hl7v3:livingSubjectBirthTime>
        <hl7v3:value value="19600422"/>
        <hl7v3:semanticsText/>
      </hl7v3:livingSubjectBirthTime>
      <hl7v3:livingSubjectId>
        <!-- German electronic healthcard card number (Serial Number) -->
        <hl7v3:value root="1.2.276.0.76.4.8" extension="1234567890"/>
        <hl7v3:semanticsText/>
      </hl7v3:livingSubjectId>
    </hl7v3:parameterList>

  </hl7v3:queryByParameter>
</hl7v3:controlActProcess>

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

```
</hl7v3:PRPA_IN201305UV02>
</soap:body>
</soap:envelope>
```

The following example shows the mapping of Czech EHIC data elements onto a PRPA_TE201305UV02 control act.



```
<hl7v3:controlActProcess classCode="CACT" moodCode="EVN">
  <hl7v3:code code="PRPA_TE201305UV02" codeSystem="2.16.840.1.113883.1.6"/>
  <hl7v3:queryByParameter>
    <hl7v3:queryId root="1.2.840.114350.1.13.28.1.18.5.999" extension="18204"/>
    <hl7v3:statusCode code="new"/>
    <hl7v3:responseModalityCode code="R" />
    <hl7v3:responsePriorityCode code="I"/>

    <hl7v3:parameterList>
      <hl7v3:livingSubjectBirthTime>
        <hl7v3:value value="19501201"/>
        <hl7v3:semanticsText/>
      </hl7v3:livingSubjectBirthTime>
      <hl7v3:livingSubjectId>
        <!-- European Health Insurance Card Serial Number -->
        <hl7v3:value root="....." extension="8020311199000000001"/>
        <hl7v3:semanticsText/>
      </hl7v3:livingSubjectId>
      <hl7v3:livingSubjectName>
        <hl7v3:value>
          <hl7v3:family>NOVAK</hl7v3:family>
          <hl7v3:given>JAN</hl7v3:given>
        </hl7v3:value>
      </hl7v3:livingSubjectName>
    </hl7v3:parameterList>
  </hl7v3:queryByParameter>
</hl7v3:controlActProcess>
```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

```

<hl7v3:semanticsText/>
</hl7v3:livingSubjectName>
<hl7v3:patientAddress>
  <hl7v3:value>
    <hl7v3:country>CZ</hl7v3:country>
  </hl7v3:value>
  <hl7v3:semanticsText/>
</hl7v3:patientAddress>
</hl7v3:parameterList>
</hl7v3:queryByParameter>
</hl7v3:controlActProcess>

```

3.2.3.1.7 e1-TXT-740 Example Response Messages

The following sample message responds to a query with the patient identifier of a patient who matches the given identity traits. The match is unique and it is a full overlap with the given query.

```

<soapenv:Envelope>
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
<hl7v3:PRPA_IN201306UV02 xmlns:xsi="...">
  <hl7v3:id root="1.2.840.114350.1.13.999.238" extension="55789"/>
  <hl7v3:creationTime value="20100304110302"/>
  <hl7v3:interactionId root="2.16.840.1.113883.1.6" extension="PRPA_IN201306UV02"/>
  <hl7v3:processingCode code="P"/>
  <hl7v3:processingModeCode code="T"/>
  <hl7v3:acceptAckCode code="NE"/>

  <hl7v3:receiver typeCode="RCV">
    <hl7v3:device classCode="DEV" determinerCode="INSTANCE">
      <hl7v3:id root="1.2.840.114350.1.13.999.567"/>
    </hl7v3:device>
  </hl7v3:receiver>

  <hl7v3:sender typeCode="SND">
    <hl7v3:device classCode="DEV" determinerCode="INSTANCE">
      <hl7v3:id root="1.2.840.114350.1.13.999.234"/>
    </hl7v3:device>
  </hl7v3:sender>

  <hl7v3:controlActProcess classCode="CACT" moodCode="EVN">

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<hl7v3:code code="PRPA_TE201306UV02" codeSystem="2.16.840.1.113883.1.6"/>
<hl7v3:subject typeCode="SUBJ">
  <hl7v3:registrationEvent classCode="REG" moodCode="EVN">
    <hl7v3:id nullFlavor="NA"/>
    <hl7v3:statusCode code="active"/>
    <hl7v3:subject1 typeCode="SBJ">
      <hl7v3:patient classCode="PAT">
        <!-- Identifier that MUST be used for subsequent requests -->
        <hl7v3:id root="1.2.276.0.76.4.8" extension="1234567890"/>
        <hl7v3:statusCode code="active"/>
        <hl7v3:patientPerson>
          <hl7v3:name/>
          <hl7v3:birthTime value="19680513"/>
        </hl7v3:patientPerson>
        <hl7v3:subjectOf1 typeCode="SBJ">
          <hl7v3:queryMatchObservation classCode="OBS" moodCode="EVN">
            <hl7v3:code codeSystem="2.16.840.1.113883.1.11.19914"/>
            <!-- Query score matching -->
            <hl7v3:value xsi:type="hl7v3:INT" value="100"/>
          </hl7v3:queryMatchObservation>
        </hl7v3:subjectOf1>
      </hl7v3:patient>
    </hl7v3:subject1>
    <hl7v3:custodian typeCode="CST">
      <hl7v3:assignedEntity classCode="ASSIGNED">
        <!-- Required element containing the homeCommunityId for the
            community responding to the request -->
        <hl7v3:id root="1.2.840.114350.1.13.99998.8734"/>
        <!-- IHE Required element defining whether the responding
            community supports the QIL transaction for this patient,
            for epSOS the required value is "NotHealthDataLocator" -->
        <hl7v3:code code="NotHealthDataLocator"
          codeSystem="1.3.6.1.4.1.19376.1.2.27.2"/>
      </hl7v3:assignedEntity>
    </hl7v3:custodian>
  </hl7v3:registrationEvent>
</hl7v3:subject>
<hl7v3:queryAck>
  <hl7v3:queryId root="1.2.840.114350.1.13.28.1.18.5.999" extension="18204"/>
  <hl7v3:queryResponseCode code="OK"/>
</hl7v3:queryAck>
</hl7v3:controlActProcess>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```
</soapenv:body>
</soapenv:envelope>
```

The following sample message responds to a request that cannot be fulfilled because of insufficient traits.

```
<soapenv:Envelope>
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
<hl7v3:PRPA_IN201306UV02 xmlns:xsi="...">
  <hl7v3:id root="1.2.840.114350.1.13.999.238" extension="55789"/>
  <hl7v3:creationTime value="20100304110302"/>
  <hl7v3:interactionId root="2.16.840.1.113883.1.6" extension="PRPA_IN201306UV02"/>
  <hl7v3:processingCode code="P"/>
  <hl7v3:processingModeCode code="T"/>
  <hl7v3:acceptAckCode code="NE"/>

  <hl7v3:receiver typeCode="RCV">
    <hl7v3:device classCode="DEV" determinerCode="INSTANCE">
      <hl7v3:id root="1.2.840.114350.1.13.999.567"/>
    </hl7v3:device>
  </hl7v3:receiver>

  <hl7v3:sender typeCode="SND">
    <hl7v3:device classCode="DEV" determinerCode="INSTANCE">
      <hl7v3:id root="1.2.840.114350.1.13.999.234"/>
    </hl7v3:device>
  </hl7v3:sender>

  <hl7v3:controlActProcess classCode="CACT" moodCode="EVN">
    <hl7v3:code code="PRPA_TE201306UV02" codeSystem="2.16.840.1.113883.1.6"/>
    <!-- Used to indicate that more attributes are required -->
    <hl7v3:reasonOf typeCode="RSON">
      <hl7v3:detectedIssueEvent classCode="ALRT" moodCode="EVN">
        <hl7v3:code code="ActAdministrativeDetectedIssueCode"
          codeSystem="2.16.840.1.113883.5.4"/>
        <hl7v3:triggerFor typeCode="TRIG">
          <hl7v3:actOrderRequired classCode="ACT" moodCode="ENV">
            <hl7v3:code code="AdditionalDemographicsRequested"
              codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1.1"/>
          </hl7v3:actOrderRequired>
        </hl7v3:triggerFor>
      </hl7v3:detectedIssueEvent>
```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

</hl7v3:reasonOf>
<hl7v3:queryAck>
  <hl7v3:queryId root="1.2.840.114350.1.13.28.1.18.5.999" extension="18204"/>
  <hl7v3:queryResponseCode code="OK"/>
</hl7v3:queryAck>
</hl7v3:controlActProcess>
</hl7v3:PRPA_IN201306UV02>
</soapenv:body>
</soapenv:envelope>

```

3.2.3.2 e1-FLD-161 Computational Dimension

3.2.3.2.1 e1-REQ-4852 epSOS Identification Service Message Specification

Related to e1-REQ-4845 epSOS IdentificationService Service Interface & Functional Specification

Related to e1-REQ-4883 epSOS Trusted Service List

The *epSOS Identification Service* MUST be used to discover a valid patient identifier from an ID assigning authority by providing given identifiers and/or demographic data that is sufficient for patient identification.

The implementation of the *epSOS Identification Service* MUST be based on the standard

HL7 IS: HL7 V3 Identification Service

and is an extension to the IHE profile XCPD: IHE Cross-Community Patient Discovery August 2009

3.2.3.2.2 e1-REQ-4853 findEntityByTraits() Operation

The *IHE XCPD Cross-Gateway Patient Discovery* transaction – as for the semantics and syntax of its content - is based on *HL7 Patient Registry Find Candidates Query* (PRPA_IN201305UV02) interaction type and used also for the IHE PIX/PDQv3 August 2009 transactions.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.2.3.2.2.1 e1-REQ-4855 Restrictions on the Use of Traits

For a *findIdentityByTraits()* request only the following traits or a subset of these MUST be used. Service providers SHOULD reject requests that contain other traits than the ones listed below.

Identity Trait	Source	Usage Convention (if provided)
LivingSubjectID	Personal ID Card	SHOULD contain zero or more living subject Id. When present, it shall contain both an assigning authority identifier (root) and individual ID (extension). If multiple subject IDs are given for the same patient, each identifier MUST be provided as a dedicated <LivingSubjectID> element.
LivingSubjectName	Personal ID Card	Family name and given name MUST both be given if no LivingSubjectID is provided. Otherwise this query parameter is optional.
LivingSubjectBirthTime	Personal ID Card	Birth date MUST be given if no LivingSubjectID is provided. Otherwise this query parameter is optional. If given this parameter MUST be encoded as "YYYY[MM[DD[HHMM[SS[S[S[S]]]]]]][+/-ZZZZ]" with year, month and day being mandatory.
LivingSubjectGender		MUST be "M" or "F"
LivingSubjectBirthPlaceAddress	Personal ID Card	SHOULD contain country and city.
PatientAddress	Personal ID Card	SHOULD contain country and city.

3.2.3.2.2.2 e1-REQ-4857 Patient Authentication

The epSOS *Identification Service* allows for the identification of a patient. If a country requires an additional authentication of its citizens when they ask for medical care in another country, this country MUST define its own authentication service.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

The *epSOS Identification Service* `findIdentityByTraits` operation only provides the mechanism for piggybacking the exchange of transparent authentication data between NCPs. This is done by using two HL7v3 *instance identifier* within a single `<LivingSubjectID>` element; one identifier is used for identifying the patient while the other one is used for authentication of the patient.

The service provider MUST be able to distinguish identifier and authentication object by their roots (assigning authorities).

3.2.3.2.2.3 e1-REQ-4858 Requested Accuracy of Matches

As the respective `<MatchCriterionList>` element is optional with the HL7 schema, it SHOULD NOT be used for the epSOS pilots. If present, the minimum requested match degree SHOULD be set to an integer value of “100”. In both cases the responding service SHOULD only respond with identity data of patients who fully match all provided traits. Returning multiple candidates’ identity trails SHOULD be avoided for privacy reasons.

3.2.3.2.2.4 e1-REQ-4859 Expected Actions

Related to e1-REQ-4870 epSOS Identification Service Errors and Warnings

Related to e1-REQ-4860 Exception Handling

Related to e1-REQ-4869 Response Message (Full Success Scenario)

The *epSOS Identification Service* provider shall respond with the `findEntityByTraits` response message containing the patient identifier that is to be used for querying the identified patient’s medical data. The *epSOS Identification Service* provider MUST verify that the requesting service user has sufficient rights to query for the identifier of the given patient. It is subject to the national security policy of the patient’s country of affiliation, how multiple matches and matches with less than 100% accuracy are handled.

In case of an error that relates to the transmission of the request or the processing of the epSOS security token, the *epSOS Identification Service* provider MUST respond with a fault message according to e1-REQ-4860.

3.2.3.2.3 e1-REQ-4872 epSOS Identification Service Protocol Requirements

Related to e1-REQ-1883 epSOS Common Message Format

The *epSOS Patient Identification Service* `FindIdentityByTraits` request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in e1-REQ-1883. Port types and bindings MUST be used as defined in the WSDL given in e1-REQ-4873. Acc. to this the epSOS `FindIdentityByTraits` operation’s request and response data MUST be contained within the message body as follows:

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

epSOS Patient Identification Service	Message Body
FindIdentityByTraits request	PRPA_IN201305UV02_Message
FindIdentityByTraits response	PRPA_IN201306UV02_Message

The request message MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in e1-REQ-4884. The response message MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in e1-REQ-4884.

3.2.3.2.3.1 e1-REQ-4873 IHE XCPD Cross Gateway Patient Discovery WSDL

```

<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions name="XCPDRespondingGateway" targetNamespace="urn:ihe:iti:xcpd:2009"
    xmlns:tns="urn:ihe:iti:xcpd:2009"
    xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:hl7="urn:hl7-org:v3">
    <wsdl:documentation>
        Example WSDL for XCPD Responding Gateway
    </wsdl:documentation>
    Optimized for epSOS; patient location queries removed
    </wsdl:documentation>
    <wsdl:types>
        <xsd:schema elementFormDefault="qualified"
            targetNamespace="urn:hl7-org:v3" xmlns:hl7="urn:hl7-org:v3">
            <!-- Include the message schema -->
            <xsd:include
                schemaLocation="../schemas/HL7V3/NE2008/multicacheschemas/PRPA_IN201305UV02.xsd"/>
        </xsd:schema>
        <xsd:schema elementFormDefault="qualified"
            targetNamespace="urn:hl7-org:v3" xmlns:hl7="urn:hl7-org:v3">
            <!-- Include the message schema -->
            <xsd:include
                schemaLocation="../schemas/HL7V3/NE2008/multicacheschemas/PRPA_IN201306UV02.xsd"/>
    </wsdl:types>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="PRPA_IN201305UV02_Message">
    <wsdl:part element="hl7:PRPA_IN201305UV02" name="Body"/>
  </wsdl:message>
  <wsdl:message name="PRPA_IN201306UV02_Message">
    <wsdl:part element="hl7:PRPA_IN201306UV02" name="Body"/>
  </wsdl:message>

  <wsdl:portType name="RespondingGateway_PortType">
    <wsdl:operation name="RespondingGateway_PRPA_IN201305UV02">
      <wsdl:input message="tns:PRPA_IN201305UV02_Message"
        wsaw:Action="urn:hl7-
org:v3:PRPA_IN201305UV02:CrossGatewayPatientDiscovery"/>
      <wsdl:output message="tns:PRPA_IN201306UV02_Message"
        wsaw:Action="urn:hl7-
org:v3:PRPA_IN201306UV02:CrossGatewayPatientDiscovery"/>
    </wsdl:operation>

  </wsdl:portType>
  <wsdl:binding name="RespondingGateway_Binding_Soap12"
    type="tns:RespondingGateway_PortType">
    <soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="RespondingGateway_PRPA_IN201305UV02">
      <soap12:operation
        soapAction="urn:hl7-org:v3:PRPA_IN201305UV02:CrossGatewayPatientDiscovery"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>

  <wsdl:service name="RespondingGateway_Service">
    <wsdl:port binding="tns:RespondingGateway_Binding_Soap12"
      name="RespondingGateway_Port_Soap12">
      <soap12:address location="https://example.org/RespondingGateway_Soap12"/>
    </wsdl:port>
  </wsdl:service>

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

</wsdl:service>
</wsdl:definitions>

3.3 e1-FLD-67 Patient Consent

3.3.1 e1-FLD-74 Conceptual Perspective

3.3.1.1 e1-FLD-158 Information Model

3.3.1.2 e1-FLD-131 Computational Dimension

3.3.1.2.1 e1-REQ-4433 Patient gives/revokes consent in "Country A"

Related to e1-REQ-4429 REQ 3.6.26 Withdrawing patient consent

Related to e1-REQ-4430 REQ 3.6.27 Self-disclosure

Related to e1-REQ-4431 REQ 3.6.28 Consent for Country B may be different from consent for Country A

Related to e1-REQ-4432 REQ 3.6.29 Patient consent regards to countries not to organisations

Patient of "Country A" at a "Point of Care (PoC)" in "Country A" prior to "Country B".

This process describes the case in which a patient is situated at PoC in his Country A and gives/revokes patient's consent prior to Country B. A patient is already identified and authenticated and a HP is also already identified, authenticated and authorised. Based on the request of a patient, a HP at PoC carries out a modification of the patient's consent in national infrastructure (national repository in CountryA). The consent modification can be "printed" and "signed" as evidence.

Highlights of this process:

Consent is given/revoked prior to Country A for Country B

Patient can give/revoke his consent for different Country B's

Attributes of Consent:

Valid from Date (YYYYMMDD)

Valid to Date (YYYYMMDD)

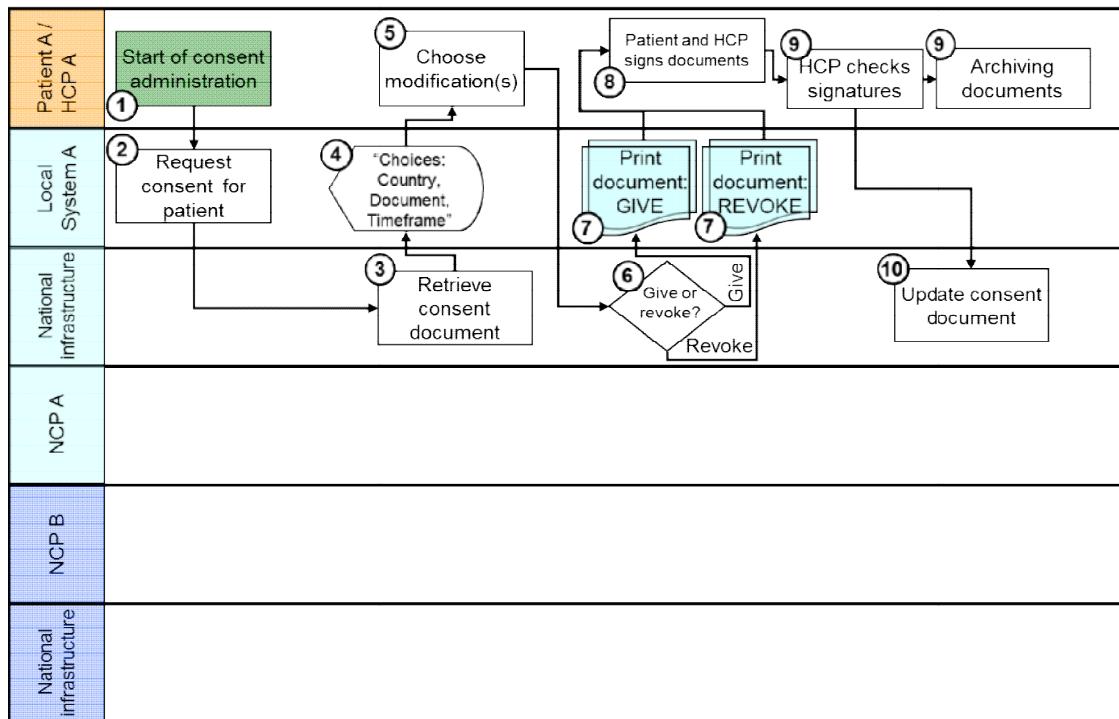
Days (NNN)

Consent Document is stored in Country A

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Consent is valid for whole Country B

This process describes Give/Revoke Consent in Country A for Country B



The process is depicted in flow diagram and consists of the following steps:

Patient is situated at PoC in Country A – start of consent management. Precondition for this process is that HP is authenticated and authorized for epSOS LSP (including check of role) and the patient is authenticated.

HP uses local system at PoC, makes a connection to national infrastructure (national repository) and requests consent for patient.

On this request the national infrastructure retrieves a consent document

Choose country, document and timeframe from national repository and send document to local system.

HP inserts patient's choice of consent document modification(s) and sends modified consent document back to national infrastructure.

The national infrastructure checks the validity of either opt-in policy or opt-out policy of modification(s) and sends to local system either document „Patient gives consent” or document „Patient revokes consent”.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

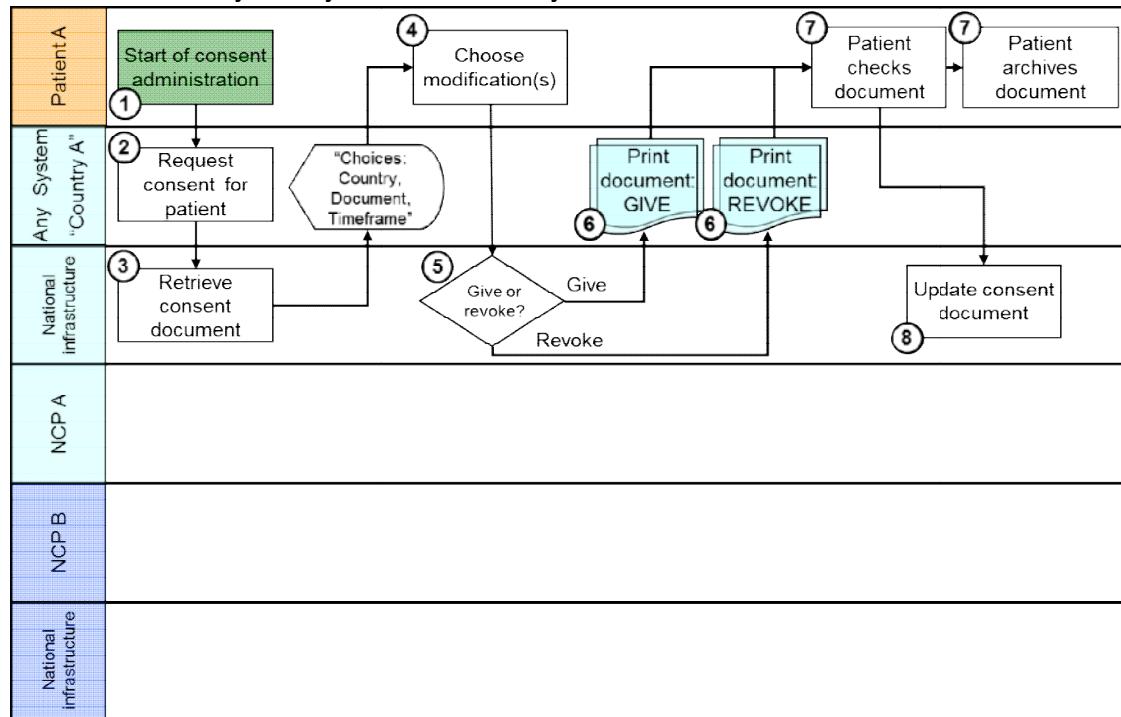
On local system the document is printed out twice (one for patient and one for HP).

The printed documents (informed consent documents) must be signed by the patient and by HP.

HP checks signature of patient (e.g. comparing with patient's passport) and archives one copy of document as an evidence of consent modification.

HP confirms the modification(s) to national infrastructure and updates the patient's consent document in national repository. **The process is finished.**

Patient of "Country A" anywhere in "Country A" wants administration of consent for "Country B"



The process is depicted in flow diagram and consists of the following steps:

Patient is situated at PoC in Country A – start of consent management. Precondition for this process is that HP is authenticated and authorized for epSOS LSP (including check of role) and the patient is authenticated.

HP uses local system at PoC, makes a connection to national infrastructure (national repository) and requests consent for patient.

On this request the national infrastructure retrieves a consent document

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Choose country, document and timeframe from national repository and send document to local system.

The national infrastructure checks the validity of either opt-in policy or opt-out policy of modification(s) and sends to local system either document „Patient gives consent” or document „Patient revokes consent”.

On local system the document is printed out twice (one for patient and one for HP).

The printed documents (informed consent documents) must be signed by the patient and by HP.

HP checks signature of patient (e.g. comparing with patient's passport) and archives one copy of document as an evidence of consent modification.

HP confirms the modification(s) to national infrastructure and updates the patient's consent document in national repository. The **process is finished**.

3.3.1.2.2 e1-REQ-4434 Patient gives/revokes consent in "Country B"

Related to e1-REQ-1970 Consent Registration

Related to e1-REQ-4832 Informing Country A about consent change in Country B

Related to e1-REQ-4676 Logging of Consent Lifecycle

Related to e1-REQ-4675 NCP Consent Checking

Related to e1-REQ-4428 REQ 3.6.25 Existence and location of patient consent

Related to e1-REQ-4429 REQ 3.6.26 Withdrawing patient consent

Related to e1-REQ-4430 REQ 3.6.27 Self-disclosure

Related to e1-REQ-4431 REQ 3.6.28 Consent for Country B may be different from consent for Country A

Related to e1-REQ-4432 REQ 3.6.29 Patient consent regards to countries not to organisations

Related to e1-REQ-4437 REQ 3.6.30 Consent for Country B modified in Country B

Related to e1-REQ-4438 REQ 3.6.31 Consent confirmation

Related to e1-REQ-4420 REQ 3.6.7 Consent in Country B for Country B

Related to e1-REQ-4421 REQ 3.6.8 Confirm consent in Country B

Related to e1-REQ-4632 epSOS ConsentService Service Interface & Functional Specification

Patient of "Country A" at a "Point of Care (PoC)" in "Country B"

This process describes the case in which a patient of Country A is situated at PoC in Country B

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

and gives/revokes patient's consent. A patient is already identified and authenticated and a HP is also already identified, authenticated and authorised for epSOS LSP and the level of trust is checked. At PoC, a HP on patient's request executes the modification of patient's consent in national infrastructure in Country A (national repository in Country A). As evidence the consent modification document is "printed out" and the document is signed by HP and by the patient. How to furnish proof in the future is an open issue (for details, see pictures and descriptions below).

Highlights of this process:

Consent is given/revoked on demand in Country B for Country B

Consent can be given/revoked only for Country B where he is staying

Attributes of Consent:

Valid from Date (YYYYMMDD)

Valid to Date (YYYYMMDD)

Days (NNN)

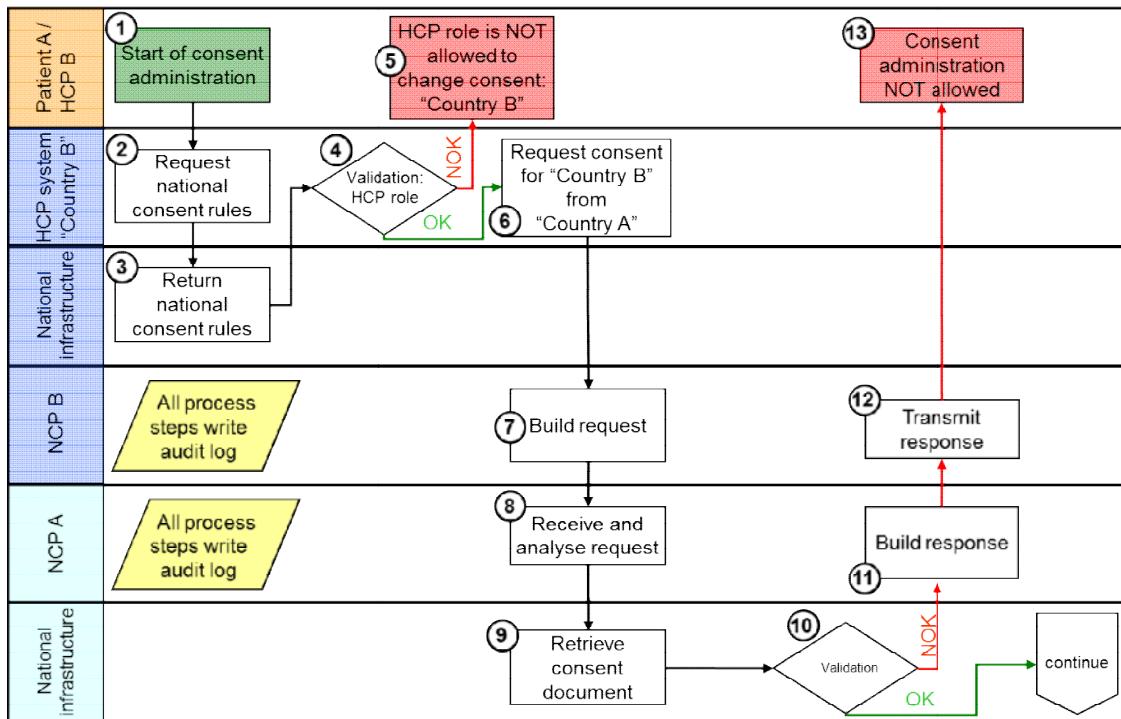
Consent Document is stored in Country A

An information has to be signed (either signing of paper, digital signature, ...)

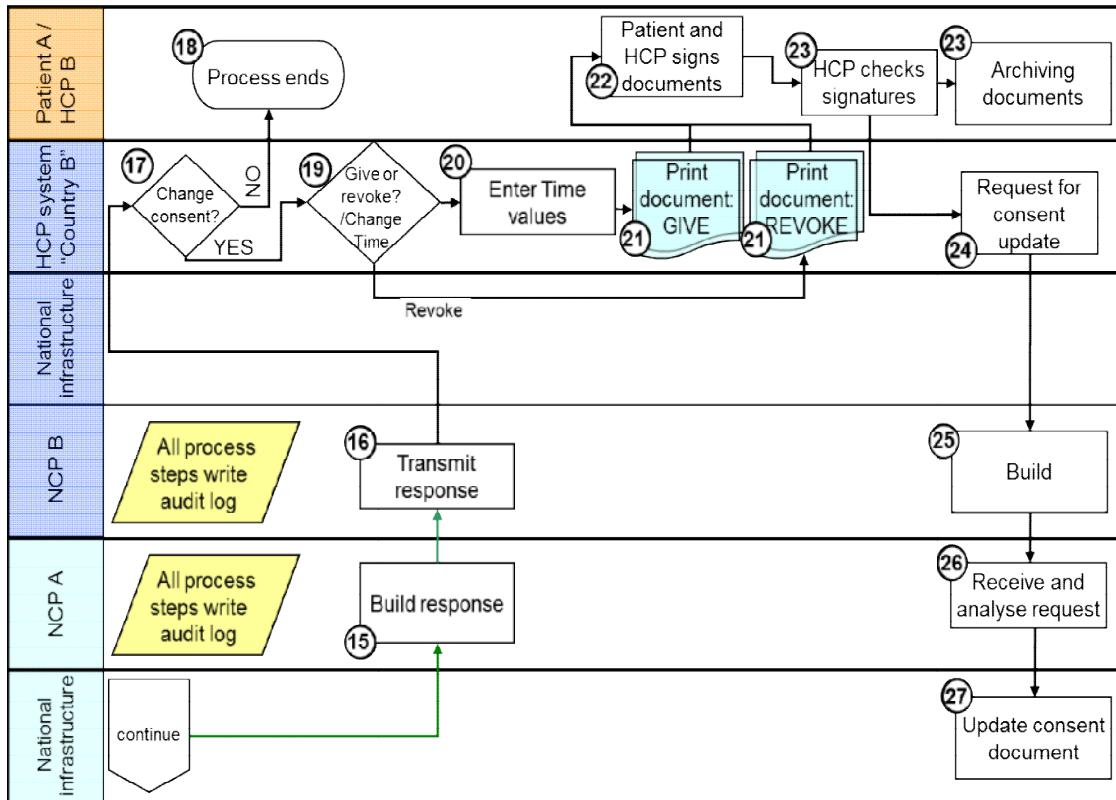
Consent is valid for whole Country B

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date: 31/01/2013	

Patient of "Country A" at a "Point of Care (PoC)" in "Country B" ("on demand")



	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



The process is depicted in flow diagrams and consists of the following steps:

Patient is situated at the PoC in Country B and asks HP for modification of patient's consent – start of consent management.

HP's local system requests national infrastructure (Country B) for national consent rules.

National infrastructure in Country B returns on request the national consent rules to the HP system.

The HP system then checks the validity of the actual role of the HP to change the patient's consent in Country B. One of the following results is returned:

OK (actual role is allowed) (continue on step 6) or

NOK (continue on step 5).

HP's actual role is not allowed to change the patient's consent in Country B – **process is finished.**

HP's system makes a request for consent for Country B from Country A and sends this request to NCP B.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The NCP B receives the request from HP system and writes a record into audit log. Then NCP B builds the request, maps it into the predefined format for Country A and transmits the request for consent to NCP A. NCP B writes a record into audit log.

NCP A receives and analyses the request from NCP B and writes an audit log.

NCP A sends a request for the consent document to the national infrastructure of Country A and writes an audit log. The actual consent document from national infrastructure of Country A will be retrieved to check the actual status of consent for Country B.

The national infrastructure in Country A checks (in the national repository) the status of patient consent for Country B and prepares the consent document. In addition to that, the level of trust and the actual role of HP B will be checked. One of the following results is returned:

patient consent for Country B is NO - Country B is not allowed – national infrastructure prepares document „Patient gives consent“ (continue on step 14) or

patient consent for Country B is YES - Country B is allowed – national infrastructure prepares document „Patient revokes consent“ (continue on step 14) or

level of trust is below the required value of Country A or actual role of HP B is not allowed to manage patient's consent (continue on step 11)

NCP A builds the response, maps it into the predefined format for Country B and sends it to NCP B. NCP A writes an audit log.

NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HP's system and writes an audit log.

HP and patient receive the result of consent for Country B and the process ends.

NCP A builds the response, maps it into the predefined format for Country B and sends it to NCP B. NCP A writes an audit log.

NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HP's system and writes an audit log.

HP and patient receive information on patient's consent status for Country B. If the patient does not want to change the consent (patient decides not to change anything) continue with step 17 else with step 18.

Process ends and the information about this will be added to audit logs in Country A and Country B.

Depending on consent details (as a result) of step 11 (Consent was given or not) the process will continue:

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

If consent was given in Country A prior to Country B or in Country B for Country B, the patient can decide if he likes to change the time parameters (proceed with step 19) or to revoke the consent (continue with step 21).

If consent was revoked or not given in Country A prior to Country B or in Country B for Country B, proceed with step 19

Enter date parameters:

Date Valid From (YYYYMMDD)

Date Valid To (YYYYMMDD)

Days (NNN)

In the case that status of patient's consent in Country B either was "NO" or patient wanted to change the timeframe, HP systems receives document "Patient gives consent" and document is "printed out" in languages of patient and of HP.

In the case that status of patient's consent in Country B was "YES" and the patient wants to revoke the consent, HP systems receives document "Patient revokes consent" and document is "printed out" in languages of patient and of HP.

Patient and HP sign documents.

HP checks signatures with identity cards (e.g. Passport, Driving Licence, etc.) and requests for consent update. The request is sent to NCP B. HP can archive one copy of document (depends on the law of Country B). The patient gets a signed copy of the physical document in his language.

HP's system sends the request for consent update to NCP B.

NCP B builds the request (or maps it to Country A) for NCP A for consent update and writes an audit log. If the patient wants to revoke his consent and the consent was prior confirmed by the patient (for details see next process description) this confirmation is deleted.

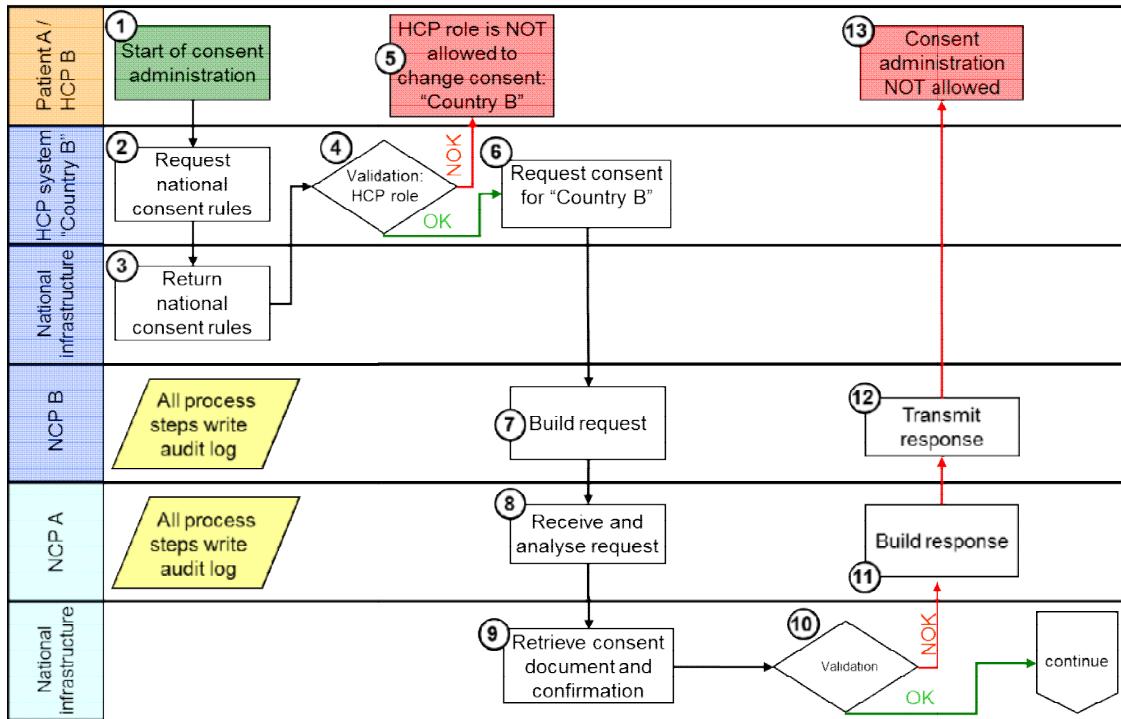
NCP A receives and analyses the request from NCP B and writes an audit log. If the patient wants to revoke his consent and the consent was prior confirmed by the patient this confirmation is deleted. NCP A sends a request for consent update to national infrastructure in Country A (national registry in Country A) and writes an audit log.

The national infrastructure in Country A updates (in national registry) the patient's consent document. The **process is finished**.

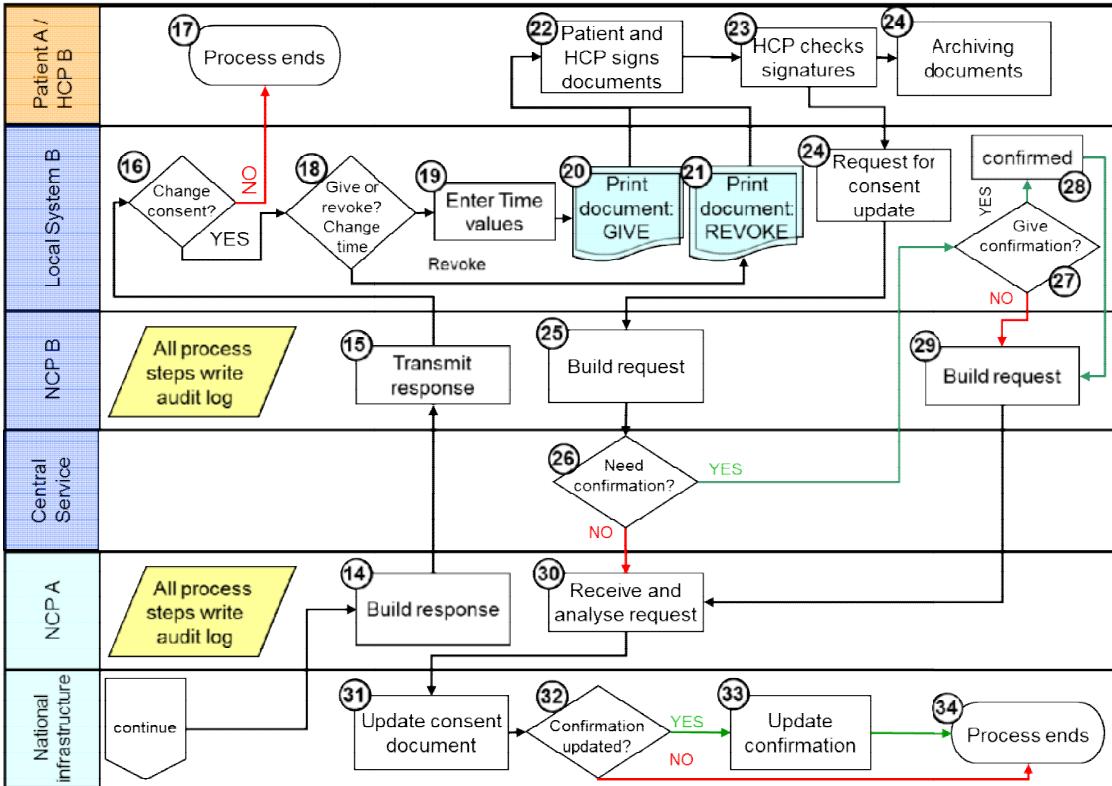
Patient of "Country A" at a "Point of Care (PoC)" in "Country B" ("on demand" including

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

confirmation)



	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



The process is depicted in flow diagrams and consists of the following steps:

Patient is situated at the PoC in Country B and asks HP for modification of patient's consent – start of consent management.

HP's local system requests national infrastructure (Country B) for national consent rules.

National infrastructure in Country B returns on request the national consent rules to the HP system.

The HP system then checks the validity of the actual role of the HP to change the patient's consent in Country B. One of the following results is returned:

- OK (actual role is allowed) (continue on step 6) or
- NOK (continue on step 5).

HP's actual role is not allowed to change the patient's consent in Country B – process is finished.

HP's system makes a request for consent for Country B from Country A and sends this request to NCP B.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

The NCP B receives the request from HP system and writes a record into audit log. Then NCP B builds the request, maps it into the predefined format for Country A and transmits the request for consent to NCP A. NCP B writes a record into audit log.

NCP A receives and analyses the request from NCP B and writes an audit log.

NCP A sends a request for the consent document to the national infrastructure of Country A and writes an audit log. The actual consent document from national infrastructure of Country A will be retrieved to check the actual status of consent for Country B.

The national infrastructure in Country A checks (in the national repository) the status of patient consent for Country B and prepares the consent document. In addition to that, the level of trust and the actual role of HP B will be checked. One of the following results is returned:

- a. patient consent for Country B is NO - Country B is not allowed – national infrastructure prepares document „Patient gives consent“ (continue on step 14) or
- b. patient consent for Country B is YES - Country B is allowed – national infrastructure prepares document „Patient revokes consent“ (continue on step 14) or
- c. level of trust is below the required value of Country A or actual role of HP B is not allowed to manage patient's consent (continue on step 11)

NCP A builds the response, maps it into the predefined format for Country B and sends it to NCP B. NCP A writes an audit log.

NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HP's system and writes an audit log.

HP and patient receive the result of consent for Country B and the **process ends**.

NCP A builds the response, maps it into the predefined format for Country B and sends it to NCP B. NCP A writes an audit log.

NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HP's system and writes an audit log.

HP and patient receive information on patient's consent status for Country B. If the patient does not want to change the consent (patient decides not to change anything) continue with step 17 else with step 20.

Process ends and the information about this will be added to audit logs in Country A and Country B.

Depending on consent details (as a result) of step 10 (Consent was given or not) the process will continue.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

If consent was given in Country A prior to Country B or in Country B for Country B, the patient can decide if he likes to change the time parameters (proceed with step 19) or to revoke the consent (continue with step 21).

If consent was revoked or not given in Country A prior to Country B or in Country B for Country B, proceed with step 19

Enter date parameters:

Date Valid From (YYYYMMDD)

Date Valid To (YYYYMMDD)

Days (NNN)

In the case that status of patient's consent in Country B either was "NO" or patient wanted to change the timeframe, HP systems receives document "Patient gives consent" and document is "printed out" in languages of patient and of HP.

In the case that status of patient's consent in Country B was "YES" and the patient wants to revoke the consent, HP systems receives document "Patient revokes consent" and document is "printed out" in languages of patient and of HP.

Patient and HP sign documents.

HP checks signatures with identity cards (e.g. Passport, Driving Licence, etc.) and requests for consent update. The request is sent to NCP B. HP can archive one copy of document (depends on the law of Country B). The patient gets a signed copy of the physical document in his language.

HP's system builds and sends the request for consent update to NCP B.

NCP B receives the request and hands it over to Central Services. This step will be logged in the audit log of Country B with the identifiers of HP B and the patient of Country A.

The Central Services layer receives the request and selects the confirmation flag for Country A. One of the following results is returned:

If patient must not give a confirmation, the process continues with step 30 or the confirmation is required

If confirmation is necessary, it has to be given explicitly. The patient has to say "Yes" (HP will tick a box and patient will confirm it). One of the following results is returned:

The patient confirms the consent.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

The confirmation is not positive, and the process continues with step 29.

Consent management process is explicitly confirmed by the patient.

NCP B builds the request (or maps it to Country A) for NCP A for consent update and writes an audit log. If the patient wants to revoke his consent and the consent was prior confirmed by the patient (for details see previous process description) this confirmation is deleted.

NCP A receives and analyses the request from NCP B and writes an audit log. If the patient wants to revoke his consent and the consent was prior confirmed by the patient this confirmation is deleted.

NCP A sends a request for consent update to national infrastructure in Country A (national registry in Country A) and writes an audit log.

If the existing confirmation state is not updated the process continues with step 34.

The national infrastructure in Country A updates (in national registry) the patient's consent document and confirmation state.

Process is finished.

3.3.1.2.3 e1-TXT-590 Messages that can occur within the consent management processes

Related to e1-REQ-2279 Patient gives/revokes consent in "Country A"

Related to e1-REQ-2280 Patient gives/revokes consent in "Country B"

As already mentioned in the preconditions of the above described processes the patient and the HP must be successfully authorised by the appropriate processes.

Regarding the single process steps the following (error) messages could show up additionally to the already described ones:

"No consent document available for this patient."

"Connection to Country A failed. Consent document and management processes are not available."

"Country B is not allowed to manage any consent of Country A."

"The entered timeframe is not valid or lies in the past."

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.3.2 e1-FLD-75 Logical Perspective

3.3.2.1 e1-REQ-4420 REQ 3.6.7 Consent in Country B for Country B

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Process Give/Revoke consent must be implemented in Country B for Country B

3.3.2.2 e1-REQ-4421 REQ 3.6.8 Confirm consent in Country B

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Consent must be confirmed in Country B for a patient from Country A if required by Country A

3.3.2.3 e1-REQ-4450 REQ 3.6.11 Audit log extraction on patient's request (Country A)

Patient in epSOS LSP has a right to know who accessed his health data and when and in which cases patient gives/revoked consent. All data are stored in national infrastructure in his country (Country A). On patient's demand, the administrator must provide patient with audit data that concerns the access to his health data or his patient's consent document.

3.3.2.3.1 e1-TXT-588 Note

An audit trail (log) is a record of the events occurring within an epSOS LSP environment (collection of individual NCPs information systems and networks). Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a NCP system or network. The logs, among the other useful goals, serve for recording the actions of users, and providing data useful for investigating malicious activity. Logs have evolved to contain information related to many different types of events occurring within networks and systems. Within an NCP, many logs contain records related to computer security; common examples of these computer security logs are audit logs that track user authentication attempts and security device logs that record possible attacks.

The ISO/IEC 27002:2005 standard formulates general requirement posed to audit logs as: audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period (has to be defined from WP 2.1) to assist in future investigations and access control monitoring.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.3.2.4 e1-REQ-4428 REQ 3.6.25 Existence and location of patient consent

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

The existence of a patient consent and its current location must be determinable within the epSOS LSP environment.

The location determination may be implemented exclusively by organisational procedures and is only invoked on an on-demand basis.

3.3.2.5 e1-REQ-4429 REQ 3.6.26 Withdrawing patient consent

Related to e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-4433 Patient gives/revokes consent in "Country A"

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Every participating nation must design, adopt, and operate procedures to enable their assigned patients (country of affiliation) to execute their right of withdrawing their consents at any time, even from abroad.

3.3.2.6 e1-REQ-4430 REQ 3.6.27 Self-disclosure

Related to e1-REQ-4433 Patient gives/revokes consent in "Country A"

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Every PN must implement organisational procedures to enable the patients to execute their granted right of self-disclosure.

3.3.2.7 e1-REQ-4431 REQ 3.6.28 Consent for Country B may be different from consent for Country A

Related to e1-REQ-4433 Patient gives/revokes consent in "Country A"

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Patients must not be forced to state their consent for the epSOS LSP services in Country A as well, when they are consenting to grant health data access for Country B. The epSOS LSP data access and exchange means regarding a full consented Country B can be independent of the consent of Country A.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.2.8 e1-REQ-4432 REQ 3.6.29 Patient consent regards to countries not to organisations

Related to e1-REQ-4433 Patient gives/revokes consent in "Country A"

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Any patient consent must be given for specific and named countries only. Furthermore, any patient's consent must be given for a Country and not particular organisations / practices within a country.

3.3.2.9 e1-REQ-4437 REQ 3.6.30 Consent for Country B modified in Country B

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Every participating PN must establish organisational procedures and technical processes to allow the modification of patient's consent in an electronically way from abroad.

3.3.2.10 e1-REQ-4438 REQ 3.6.31 Consent confirmation

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

A PN may require a confirmation of the consent which was given prior to Country B in Country A or a confirmation on demand in Country B for Country B.

3.3.2.11 e1-REQ-4675 NCP Consent Checking

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

NCP-A must check patient consent according to its national policy (rules for health data disclosure). To minimize data processing, this checking should be done before any semantic processing.

3.3.2.12 e1-REQ-4674 Electronic Format of Patient Consent

2 formats of consent should be able to be transmitted:

- 1) A signed XML based SAML assertion. This consent is created by the NCP B and A, on the fly and added with the transaction for the exchange;
- 2) A PDF document. This consent is the original document created when the prior consent was given by the patient. It persists under the country A side.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.2.13 e1-REQ-4676 Logging of Consent Lifecycle

Related to e1-REQ-4942 Discard() Operation Security and Audit Considerations

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Related to e1-REQ-4941 Put() Operation Security and Audit Considerations

Lifecycle of the consent must be logged in a way that the legitimacy of each request can be constructed in retrospect.

3.3.2.14 e1-REQ-4604 Rejection of Consent change

Related to e1-REQ-4632 epSOS ConsentService Service Interface & Functional Specification

NCP-A MAY decide to reject the consent given in country B.

3.3.2.15 e1-REQ-4831 Consent time frame validity

Related to e1-REQ-4841 General Considerations for Successful Service Operations

Country A shall calculate patient consent time frame validity.

3.3.2.16 e1-REQ-4832 Informing Country A about consent change in Country B

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

If previous consent in country A does not exist and the patient gives his/her consent status explicitly (in a digital format) in country B, then country B should inform country A of this new consent.

3.3.2.17 e1-FLD-133 Information Model

3.3.2.18 e1-FLD-132 Computational Dimension

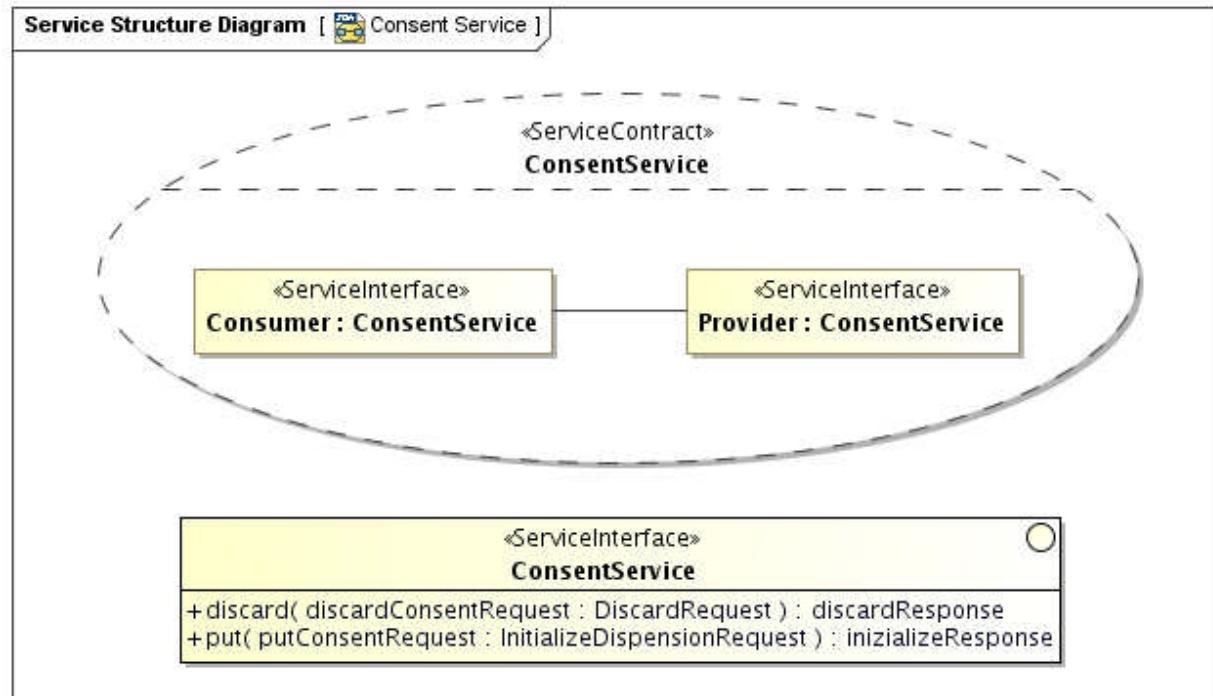
3.3.2.18.1 e1-REQ-4632 epSOS ConsentService Service Interface & Functional Specification

Related to e1-REQ-4434 Patient gives/revokes consent in "Country B"

Related to e1-REQ-4604 Rejection of Consent change

Related to e1-REQ-4844 epSOS ConsentService Service Interface & Functional Specification

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013



Operation put()

Description Notify the patient's country of affiliation on a consent newly given in the country of care

Requestor Consuming Gateway at NCP-B

Input Message putConsentRequest

Body Information on the newly given consent

Security Token X.509 Gateway Certificate

epSOS HCP Identity Assertion
epSOS Treatment Relationship Confirmation Assertion

Output putConsentResponse

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Message in successful Case	Body Security Token	Status of the consent (accepted/rejected) X.509 Gateway Certificate
Precondition of success scenario	The requestor is able to locate the service provider The certificate of the NCP-A gateway is available to the requestor. The requestor is able to verify the certificate of the NCP-A gateway. The NCP-A gateway is able to verify the requestor's certificate. An HCP identity assertion has been issued by NCP-B and is available to the requestor The NCP-A gateway is able to verify the validity of the HCP identity assertion NCP-A and NCP-B agreed on a common ID for referencing to the patient An TRC assertion has been issued by NCP-B and is available to the requestor The NCP-A gateway is able to verify the validity of the TRC assertion	
Main success scenario	Actions of the epSOS Consent Service provider: validate the message signature verify HCP identity assertion and TRC assertion extract the consent infomation from the message body enforce national security policy and (if available) patient privacy policy perform activities acc. to country-A consent regulations sign the response message and send it to the requestor	
Fault Conditions		

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Operation discard()

Description Notify the patient's country of affiliation on the revocation of a consent
 (revocation only affects the recent country of care)

Requestor Consuming Gateway at NCP-B

Input Message discardConsentRequest

Body Empty

Security Token X.509 Gateway Certificate

epSOS HCP Identity Assertion
 epSOS Treatment Relationship Confirmation
 Assertion

Output Message in discardConsentResponse

successful Case Body Status of the consent revocation
 (accepted/rejected)

Security Token X.509 Gateway Certificate

Precondition of success The requestor is able to locate the service provider

scenario The certificate of the NCP-A gateway is available to the requestor.

The requestor is able to verify the certificate of the NCP-A gateway.

The NCP-A gateway is able to verify the requestor's certificate.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

An HCP identity assertion has been issued by NCP-A and is available to the requestor

The NCP-A gateway is able to verify the validity of the HCP identity assertion

NCP-A and NCP-B agreed on a common ID for referencing to the patient

An TRC assertion has been issued by NCP-A and is available to the requestor

The NCP-A gateway is able to verify the validity of the TRC assertion

Main success scenario	Actions of the epSOS Consent Service provider: validate the message signature verify HCP identity assertion and TRC assertion verify that the patient has given consent to epSOS and that the consent is valid enforce national security policy and (if available) patient privacy policy perform activities acc. to country-A consent regulations sign the response message and send it to the requestor
Fault Conditions	<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>

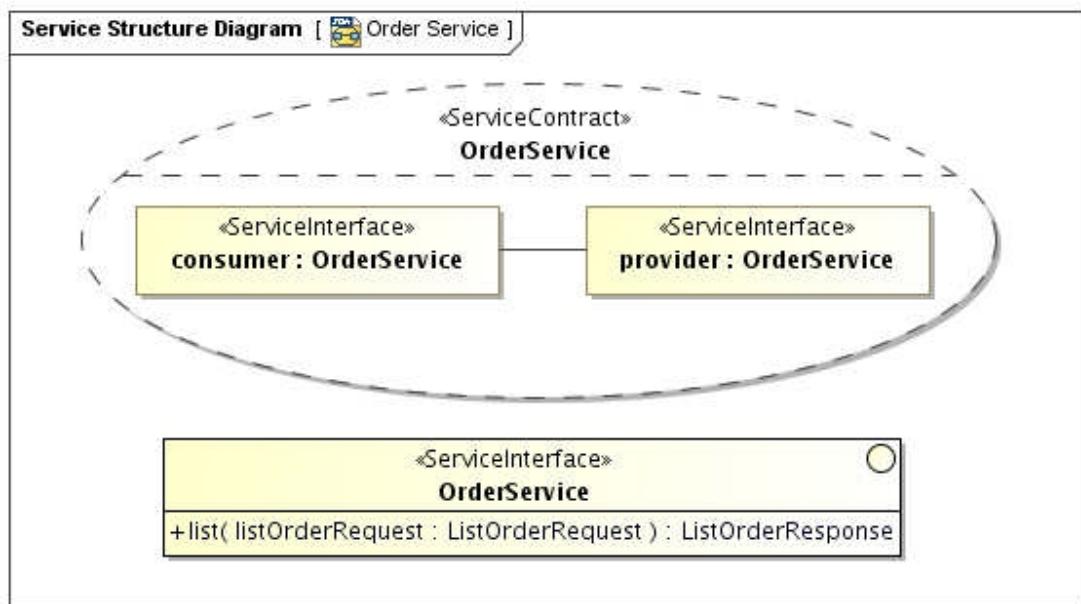
	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.2.18.2 e1-REQ-4844 epSOS ConsentService Service Interface & Functional Specification

Related to e1-REQ-4632 epSOS ConsentService Service Interface & Functional Specification

Related to e1-REQ-4841 General Considerations for Successful Service Operations

Related to e1-REQ-4930 epSOS Consent Service Message Specification



Operation: put

Operation put()

Description Notify the patient's country of affiliation on a consent newly given or revoked in the country of care. The consent status modification only applies to the country of care.

Requestor Consuming Gateway at NCP-B (service consumer at the country of care)

Input putConsentRequest

Message	Body	(1) Information on the newly given or revoked consent
---------	------	---

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

(2) Optional: signed (scanned) consent document

Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion [O]
Output Message in successful Case	putConsentResponse
Body	Status of the consent (given/revoked)
Security Token	[PT] X.509 NCP-A service certificate
Precondition of success scenario	In addition to the requirements stated in e1-REQ-4841 the following preconditions MUST be met for successful processing: Service consumer and service provider share a common identifier for the patient The patient has confirmed in the consent status change
Main success scenario	Actions of the epSOS Consent Service provider: Validate the authenticity of the service consumer Verify HCP identity assertion Verify that the requested status change is allowed by country-A security policies Apply the consent status change for the country of care Sign the success indicator and send it to the requestor
Fault Conditions	Preconditions for a success scenario are not met Security policy violation (e.g. the HCP's role is not permitted to mediate consent changes) A patient authentication is required [1] (e.g. by signing the consent document)

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Country-A legislation requires that a scanned consent document is provided with the request [2]

Temporary failure (e.g. service provider is temporarily unable to access an internal service)

[1] It is assumed that the PN policies on giving consent from abroad will evolve over time and MAY even be different for different partner relationships. In order to allow for high flexibility, epSOS allows each country A role to decide (even on a per-request basis) which safeguards it requires in order to accept a consent status change from abroad. Therefore this failure is to be interpreted as a notification on the country A policy for consent status changes from abroad (The alternative would have been a static configuration or a dedicated operation for querying a country's consent policy).,

[2] see previous footnote

Operation: discard

Operation	Discard()
Description	Notify the patient's country of affiliation on an erroneous consent status change notification, in order to allow it to roll back any changes made on its internal data that were triggered by the erroneous notification
Requestor	Consuming Gateway at NCP-B (service consumer at the country of care)
Input Message	discardConsentRequest
Body	(1) Identifier of the consent status document that is to be discarded
Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Output Message in successful Case	discardConsentResponse
	Body Notification on the result of the roll back request
	Security Token [PT] X.509 NCP-A service certificate
Precondition of success scenario	In addition to the requirements stated in e1-REQ-4841 the following preconditions MUST be met for successful processing: The service consumer has previously triggered a consent change and is responsible for the consent document that is to be discarded
Main success scenario	<p>Actions of the epSOS Consent Service provider:</p> <p>Validate the authenticity of the service consumer</p> <p>Verify HCP identity assertion</p> <p>Extract the consent document id from the message body and ensure that this consent status change was previously triggered by the identified HP</p> <p>Enforce national security policy and (if available) patient privacy policy</p> <p>Trigger the roll back of the consent giving/revocation</p> <p>Sign the success notification and send it to the requestor</p>
Fault Conditions	<p>Preconditions for a success scenario are not met</p> <p>Country-A legislation does not allow for discarding a consent; a new consent is required</p> <p>The HP was not the original mediator of the identified consent document</p> <p>The identified document is not known</p> <p>Temporary failure (e.g. service provider is temporarily unable to access an internal service)</p>

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.3 e1-FLD-167 Implementable Perspective

3.3.3.1 e1-FLD-168 Information Dimension

3.3.3.1.1 e1-REQ-4881 epSOS Consent Document and Code

epSOS Consumer Document	Display Name	Coding Scheme	Node Representation
Consent	Privacy Policy Acknowledgement Document	2.16.840.1.113883.6.1	57016-8

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.3.1.2 e1-FLD-187 Put() Operation Request/Response Messages

3.3.3.1.2.1 e1-REQ-4935 Request Message

Related to e1-REQ-1983 Structured Information and Semantic Compliance

The put() request MUST be initiated by an HP in the country of care for handing over a consent status change notifications to the patient's country of affiliation. Each consent status change notification MUST consist of a *Patient Privacy Consent Acknowledgment Document* acc. to section 5.1 of IHE ITI TF-3 October 2008. The *Scanned Document Part* acc. to section 5.2 of IHE ITI TF-3 October 2008 is optional.

The epSOS Consent Service Put() Request message corresponds to the *IHE Provide And Register DocumentSet* transaction (ITI-41) request message as profiled in IHE XDR. The fields defined for the *ProvideAndRegisterDocumentSetRequest* message MUST be used as follows:

Element Name	epSOS Usage Convention
SubmitObjectsRequest	Container that can be used to provide the metadata for the transmitted documents, the submission set and the associations between documents (see below).
../RegistryObjectList	Container that contains a single element that holds the metadata for the transmitted consent document.
.../ExtrinsicObject	A single Patient Privacy Consent Acknowledgment Document MAY be transmitted. The element holds all metadata for this document. Metadata and classifications MUST comply with sections 5.1 and 5.2 of IHE ITI TF3 October 2008. The scanned document option MAY be used for transmitting a scanned consent document.
.../Document	base64encoded data for the consent document being submitted to the service provider. The element also includes the document id attribute (rimext:Document/@id) of type xsd:anyURI to match the document ExtrinsicObject id in the metadata and providing the necessary linkage. The base64 encoded document content MAY be encrypted. How encryption is applied and how the encryption key is negotiated should be subject to an additional specification on advanced security safeguards.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The service consumer MAY wrap the provided document as a single IHE XDS submission set IHE ITI TF-2a August 2009 or assign it to a folder. The service consumer SHOULD ignore these groupings and MUST ignore all associations between documents and folders or submission sets.

For each consent document (either with or without a scanned paper consent document attached) the following set of metadata MUST be provided acc. to IHE BPPC IHE ITI TF-3 October 2008:

Metadata element	Binding	Slot Value
id	Attribute	Identifier of the document. This identifier MUST be the same for and .
contentType	Attribute	MUST be "text/xml"
objectType	Attribute	MUST be set acc. to section 4.3.1.2 of IHE ITI TF-3 October 2008
Status	Attribute	MUST be "urn:oasis:names:tc:ebxml-regrep>StatusType:Approved"
creationTime	rim:Slot	MUST be given for XDR compatibility. SHOULD be ignored by the service provider.
languageCode	rim:Slot	MUST be given for XDR compatibility. SHOULD be ignored by the service provider.
sourcePatientID	rim:Slot	MUST be of the same value as \$XDSDocumentEntry.PatientId (see below)
healthcareFacilityTypeCode	classification	MUST be provided for XCF compatibility and correct addressing. Value MUST be set to ISO 3166-1 alpha-2 country code of the addressed PN.
practiceSettingCode	classification	MUST be provided for XDR compatibility but MAY be ignored by the service consumer. Value MUST be set to "Not Used".
confidentialityCode	classification	MUST be provided for XDR compatibility but MAY be ignored by the service consumer.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

		Value SHOULD be set to "N", as long as the Minimal Metadata Profile is not published.
\$XDSDocumentClassCode	classification	MUST be "57016-8"
\$XDSDocumentFormatCode	classification	MUST be "urn:ihe:iti:bppc-sd:2007" if a scanned consent PDF document is included and "urn:ihe:iti:bppc:2007" otherwise. As code system "1.3.6.1.4.1.19376.1.2.3" MUST be used.
\$XDSDocumentEventCode	classification	MUST refer to the privacy policy identifier that corresponds to the given consent (see table below). The code system MUST be set to "1.3.6.1.4.1.12559.11.10.1.3.2.4.1".
\$XDSDocumentEntry.PatientId	External identifier	Equals to the patient identifier that was provided by the epSOS <i>Identification Service</i> (encoded as HL7 v3 II data type)
\$XDSDocument.EntryUUID	External identifier	MUST refer to the UUID of the corresponding element.
\$XDSDocument.UniqueId	External identifier	MUST refer to the OID of the CDA document that is included within the element.

Other metadata than the ones listed above SHOULD NOT be provided by the service provider. If given they MUST be ignored by the service consumer.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

For epSOS the following privacy policy identifiers are defined:

Privacy Policy Identifier	Value	Description
1.3.6.1.4.1.12559.11.10.1.3.2.4.1.1	Opt-in	The patient gave consent that allows HPs of the current country of care to access his medical data by the means of epSOS.
1.3.6.1.4.1.12559.11.10.1.3.2.4.1.2	Opt-out	The patient revoked any consent that allowed HPs of the current country of care to access his medical data by the means of epSOS.

3.3.3.1.2.2 e1-REQ-4936 Response Message (Full Success Scenario)

Related to e1-REQ-4934 Expected Actions

If the *epSOS Consent Service* provider is able to decode the received consent document and to properly process the consent codes and the (optional) scanned document it MUST respond with an *ebXML Registry Response* with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

```
<rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
</rs:RegistryResponse>
```

3.3.3.1.2.3 e1-TXT-763 Example Request Message

The following excerpt from a *epSOS Consent Service Put()* Request message shows the transmission of a Patient Privacy Consent Acknowledgment Document (without scanned document part). Only the consent specific parts of the message are shown.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
<xds:ProvideAndRegisterDocumentSetRequest xmlns=...>
  <lcm:SubmitObjectsRequest>
    <rim:RegistryObjectList>

      <!-- IHE BPPC compliant consent document -->
      <rim:ExtrinsicObject id="epSOS Consent">
```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
 status="urn:oasis:names:tc:ebxml-regrep>StatusType:**Approved**"
 mimeType="text/xml"
 isOpaque="false">

<!-- Metadata not shown here -->

```

<rim:Classification id="urn:uuid:466535d7-2c81-4ee7-af62-a1f956e10ff7"
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
classifiedObject="epSOS Consent"
nodeRepresentation="Consent"
<rim:Slot name="codingScheme">
  <rim:ValueList>
    <rim:Value>Connect-a-thon classCodes</rim:Value>
  </rim:ValueList>
</rim:Slot>
<rim:Name>
  <rim:LocalizedString xml:lang="en-us" charset="UTF-8"
    value="57016-8"/>
</rim:Name>
<rim:Description/>
<rim:VersionInfo versionName="1.1"/>
</rim:Classification>

<rim:Classification id="urn:uuid:..."
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
classificationScheme="urn:oid: 1.3.6.1.4.1.19376.1.2.3"
classifiedObject="epSOS Consent"
nodeRepresentation="urn:ihe:iti:bppc:2007" >
<rim:Slot name="codingScheme">
  <rim:ValueList>
    <rim:Value>Connect-a-thon formatCodes</rim:Value>
  </rim:ValueList>
</rim:Slot>
<rim:Name>
  <rim:LocalizedString xml:lang="en" charset="UTF-8"
    value="57016-8"/>
</rim:Name>
<rim:Description/>
<rim:VersionInfo versionName="1.1"/>
</rim:Classification>
  
```

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

```

<rim:Classification id="...."
    classificationScheme="urn:oid:1.3.6.1.4.1.12559.11.10.1.3.2.4.1"
    classifiedObject="epSOS Consent"
    nodeRepresentation="urn:oid:1.3.6.1.4.1.12559.11.10.1.3.2.4.1.1" >
<rim:Slot name="codingScheme">
    <rim:ValueList>
        <rim:Value>epSOS Consent Code</rim:Value>
    </rim:ValueList>
</rim:Slot>
<rim:Name>
    <rim:LocalizedString xml:lang="en-us" charset="UTF-8"
        value="Opt-in"/>
</rim:Name>
<rim:Description/>
<rim:VersionInfo versionName="1.1"/>
</rim:Classification>

    <!-- Unique ID -->
    <rim:ExternalIdentifier
        id="urn:uuid:c67e3a92-5300-448d-9af2-0a37e9f129bf"
        objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
        identificationScheme="urn:uuid:2e82c1f6-a085-4c72-
9da3-8640a32e42ab"
        value="1.42.20100103225206.3.3" registryObject="epSOS
Consent">
        <rim:Name>
            <rim:LocalizedString xml:lang="en-us"
charset="UTF-8"
                value="XDSDocumentEntry.uniqueId"/>
        </rim:Name>
    </rim:ExternalIdentifier>

    <!-- Document contents, before MTOM optimization -->
    <rimext:Document>
        UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUUhEUzhi....
    </rimext:Document>
</rim:ExtrinsicObject>

    <!-- The SubmissionSet is necessary as a 'wrapper' around
metadata

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

```

        submissions -->
<rim:RegistryPackage id="SubmissionSet01"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:RegistryPackage">

    <!-- submission set metadata not shown here -->

    </rim:RegistryPackage>

    <!-- This labels the above RegistryPackage as a
SubmissionSet object -->
    <rim:Classification classifiedObject="SubmissionSet01"
        classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-
b4633d873bdd" id="ID_446196_1"
        objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"/>

    <!-- The DocumentEntry (ExtrinsicObject) included must be
part of the
        SubmissionSet. The following association make this so
-->
    <rim:Association
        associationType="urn:oasis:names:tc:ebxml-
regrep:AssociationType:HasMember"
        sourceObject="SubmissionSet01"
        targetObject="epsOS Consent"
        id="ID_446196_2"
        objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Association">
        <rim:Slot name="SubmissionSetStatus">
            <rim:ValueList>
                <rim:Value>Original</rim:Value>
            </rim:ValueList>
        </rim:Slot>
    </rim:Association>
</rim:RegistryObjectList>

</lcm:SubmitObjectsRequest>
</xds:ProvideAndRegisterDocumentSetRequest>
</soapenv:Body>
</soapenv:Envelope>
```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.3.3.1.2.4 e1-TXT-764 Example Response Messages

The following example shows a possible positive response to the request given in e1-TXT-763:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header>...</soapenv:header>
<soapenv:Body>
  <rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" />
</soapenv:Body>
</soapenv:Envelope>
```

The following example shows a possible negative response to the request given in e1-TXT-763:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header>...</soapenv:header>
<soapenv:Body>
  <rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
    <rs:RegistryErrorList>
      <rs:RegistryError
        severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Failure"
        errorCode="...."
        codeContext="Policy Violation"
        location="" />
    </rs:RegistryErrorList>
  </rs:RegistryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

3.3.3.1.3 e1-FLD-188 Discard() Operation Request/Response Messages

3.3.3.1.3.1 e1-REQ-4937 Request Message

The epSOS Consent Service discard() request MUST be initiated by an HP in the country of care (country B) for deleting a previously transmitted BPPC consent document at the patient's country of affiliation (country A).

The respective request message corresponds to the ebXML 3.0 RemoveObjectsRequest message. The fields defined for the ebXML 3.0 RemoveObjectsRequest MUST be used as defined in IHE XDS Metadata Update:

Element Name	epSOS Usage Convention
ObjectRefList	Wrapper on the consent that has been erroneously sent to country A
./ObjectRef	For each of the consent document, submission set and submission set association to discard there MUST be a single ObjectRef element
@id	The id-attribute MUST refer to the object identifier as given in the metadata of the object to be deleted.

In order to completely discard a previously transmitted consent, all of the following objects MUST be referenced in the :

Consent document (with or without scanned consent)

Submission set

Associations between consent document and the submission set

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.3.3.1.3.2 e1-REQ-4938 Response Message (Full Success Scenario)

Related to e1-REQ-4944 Expected Actions

If the *epSOS Consent Service* provider is able to decode the received consent document IDs and to properly process the request, it responds with an *ebXML Registry Response* with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success".

```
<rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
</rs:RegistryResponse>
```

3.3.3.1.3.3 e1-TXT-765 Example Request Message

Following an example on the use of the ebXML RemoveObjectsRequest message for discarding erroneously transmitted epSOS documents:

```
<soapenv:Envelope xmlns...>
  <soapenv:Header>
    ...
  </soapenv:Header>
  <soapenv:Body>
    <lcm:RemoveObjectsRequest
      xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
      xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
      <ObjectRefList xmlns="urn:oasis:names:tc:ebxml-
      regrep:xsd:rim:3.0">

        <!-- epSOS BPPC consent document -->
        <ObjectRef id="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
        01d7b6b0f481"/>

        <!-- SubmissionSet -->
        <ObjectRef id="urn:uuid:cafddedeb-d13c-4242-b27b-
        cf2bf9644748"/>

      </ObjectRefList>
    </lcm:RemoveObjectsRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.3.3.1.3.4 e1-TXT-766 Example Response Messages

The following example shows a possible positive response to the request given in e1-TXT-765:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header>...</soapenv:Header>
<soapenv:Body>
  <rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
  </rs:RegistryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

The following example shows a possible negative response to the request given in e1-TXT-765:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header>...</soapenv:Header>
<soapenv:Body>
  <rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
  <rs:RegistryErrorList>
    <rs:RegistryError
      severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"
      errorCode="...."
      codeContext="No Match"
      location="" />
  </rs:RegistryErrorList>
  </rs:RegistryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.3.1.4 e1-FLD-189 epSOS Consent Service Errors and Warnings

3.3.3.1.4.1 e1-REQ-4939 Put() Operation Errors and Warnings

Related to e1-REQ-4934 Expected Actions

If the service provider wants to respond with further information on the processing of the transmitted consent or with a non-critical warning it SHOULD include an additional `<RegistryErrorList>` element. The severity MUST be set to “urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning”:

```

<rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
<rs:RegistryErrorList>
    <rs:RegistryError
        severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning"
        errorCode="...."
        codeContext="Processing deferred"
        location="" />
</rs:RegistryErrorList>
</rs:RegistryResponse>

```

The following warning messages and codes are defined:

Condition and Severity	Message	Code	Action to be taken
Consent document was received but will not be processed automatically	Processing deferred	2201	None

If the *epSOS Consent Service* provider is able to decode the received message but the processing of the contained consent failed, it responds with an *ebXML Registry Response* that contains a respective status indicator (see below). The response MUST contain a `RegistryErrorList` element that indicates the failure condition.

The response status MUST be set to:

“urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”.

A failure location MUST NOT be given. The severity of each registry error message MUST be set to:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

"urn:oasis:names:tc:ebxml-regrep>ErrorSeverityType:Error".

Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element.

epSOS Consent Service allows for all of the XDS-b error messages defined in Table 4.1-11 of IHE ITI TF-3 October 2008. In addition the following error codes are defined:

Condition and Severity	Message	Code	Action to be taken
Country A does not allow for consent giving or revoking in other countries	Policy Violation	4705	-
Country A requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation).	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechanism (e.g. smartcard) and re-issue the request with the respective identity assertion.
The provided privacy policy identifier is not supported by country A.	Unknown policy	4706	The HP SHOULD ask for a more basic consent and re-issue the request.
Country-A requires for a general consent for epSOS that MUST have been given in country A before more specific consents can be accepted.	No consent	4701	The patient MAY use the epSOS help desk of country A to give the general epSOS consent. The HP SHOULD re-issue the request after the general consent has been set operational.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.3.1.4.2 e1-REQ-4940 Discard() Operation Errors and Warnings

Related to e1-REQ-4944 Expected Actions

If the *epSOS Consent Service* provider is able to decode the received consent document IDs but the deprecating of the consent document failed, it MUST respond with an *ebXML Registry Response* that contains a respective status indicator (see below). The response MUST contain a *RegistryErrorList* element that indicates the failure condition.

The response status MUST be set to “urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”. A failure location MUST NOT be given. The severity of each registry error message MUST be set to “urn:oasis:names:tc:ebxml-regrep>ErrorSeverityType:Error”. Multiple registry error messages MAY be included within a single element. epSOS Consent Service allows for all of the XDS-b error messages defined in Table 4.1-11 of IHE ITI TF-3 October 2008. In addition the following error codes are defined:

Condition	Message	Code	Action to be taken
No matching consent document was found	No match	4105	The HP SHOULD verify the OID of the consent and re-issue the request.
Request is rejected because the issue is not the author of the document	Insufficient rights	4703	HPO SHOULD ensure that the discard request is issued by the same person who accepted the original consent. If consent was given at another HPO the patient MUST request for discarding at this HPO.
Country A does not allow for deprecating consent documents. This MAY be the case for countries that manage consents within their national infrastructures where the NCP does not have sufficient rights to undo changes on internal data or where undo operations are generally not supported.	Deprecation rejected	4109	In order to “simulate” the deprecation of a consent the HP SHOULD ask the patient for a reverse consent (e.g. Opt-Out in case of an erroneously sent Opt-In consent) and send this consent to country A by using the put() operation.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.3.1.5 e1-FLD-190 epSOS Consent Service Security Audit Considerations

3.3.3.1.5.1 e1-REQ-4941 Put() Operation Security and Audit Considerations

Related to e1-REQ-4676 Logging of Consent Lifecycle

Related to e1-REQ-1838 epSOS HCP Assurance Audit Schema

Related to e1-REQ-1839 epSOS Patient Privacy Audit Schema

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in e1-REQ-1838. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in e1-REQ-1839.

The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event
Requesting Point of Care	R / X	HPO that issued the original request. This category MUST be filled by the service consumer. It MUST NOT be provided by the service provider.
Human Requestor	R	HP that triggered the request
Source Gateway	R	Service consumer node address at the country of Care
Target Gateway	R	Service provider node address at the country of the patient's affiliation
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	R	Patient
Event Target	R	Subject to the Query
Error Message	O	Only used in case that the request handling was not completed successfully

For the Event Target Category the following fields MUST be provided:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "4" (Resource)
ParticipantObjectIDTypeCode	R	MUST be "12" (URI)
ParticipantObjectID	R	MUST be string-encoded UUIDs of the provided documents

3.3.3.1.5.2 e1-REQ-4942 Discard() Operation Security and Audit Considerations

Related to e1-REQ-4676 Logging of Consent Lifecycle

Related to e1-REQ-1838 epSOS HCP Assurance Audit Schema

Related to e1-REQ-1839 epSOS Patient Privacy Audit Schema

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in e1-REQ-1838. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in e1-REQ-1839.

The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event
Requesting Point of Care	R / X	HPO that issued the original request. This category MUST be filled by the service consumer. It MUST NOT be provided by the service provider.
Human Requestor	R	HP that triggered the request
Source Gateway	R	Service consumer node address at the country of Care
Target Gateway	R	Service provider node address at the country of the patient's affiliation
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Patient	R	Patient
Event Target	R	Reference to the discarded document
Error Message	O	Only used in case that the request handling was not completed successfully

For the Event Target Category the following fields MUST be provided:

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "4" (Resource)
ParticipantObjectDataLifeCycle	R	MUST be "14" (logical deletion)
ParticipantObjectIDTypeCode	R	MUST be "12" (URI)
ParticipantObjectID	R	MUST be string-encoded UUIDs of the discarded documents

3.3.3.2 e1-FLD-185 Computational Dimension

3.3.3.2.1 e1-REQ-4930 epSOS Consent Service Message Specification

Related to e1-REQ-4844 epSOS ConsentService Service Interface & Functional Specification

Related to e1-REQ-4883 epSOS Trusted Service List

The epSOS Consent Service MUST be used to send an identified patient's eConsent data from the country of care (Country B) to the patient's country of affiliation (Country A). Both countries are represented by their respective NCPs.

The implementation of the epSOS Consent Service is based on the following standards:

ebRIM: OASIS/ebXML Registry Information Model v3.0 OASIS ebRIM 3.0

ebRS: OASIS/ebXML Registry Services Specifications v3.0 OASIS ebRS 3.0

MTOM: SOAP Message Transmission Optimization Mechanism W3C MTOM

XOP: XML-binary Optimized Packaging W3C XOP

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

and is compliant with the IHE profiles:

XDR: IHE Cross-Enterprise Reliable Exchange IHE XDR

BPPC: IHE Basic Patient Privacy Consent IHE ITI TF-3 October 2008

For discovery and localisation of the epSOS *Consent Service* instance that is responsible for providing access to the identified patient's data see e1-REQ-4883.

3.3.3.2.1.1 e1-REQ-4933 Put() Operation

The epSOS *Consent Service* put() operation is implemented by the *IHE Provide And Register DocumentSet* transaction (ITI-41) as described in IHE XDR.

3.3.3.2.1.1.1 e1-REQ-4934 Expected Actions

Related to e1-REQ-4860 Exception Handling

Related to e1-REQ-4939 Put() Operation Errors and Warnings

Related to e1-REQ-4936 Response Message (Full Success Scenario)

The epSOS *Consent Service* provider shall respond to an PutRequest message with the PutResponse message containing a success indicator.

The epSOS *Consent Service* provider MUST verify that the requesting service user has sufficient rights to submit a consent for the identified patient.

In case of an error that relates to the transmission of the request or the processing of the epSOS security token, the epSOS *Consent Service* provider MUST respond with a fault message according to e1-REQ-4860.

3.3.3.2.1.2 e1-REQ-4943 Discard() Operation

The epSOS *Consent Service* discard() operation MUST be used to deprecate a previously transmitted consent. It is implemented by the ebXML RemoveObjectsRequest registry operation as profiles in the IHE Draft Profile on XDS Metadata Update.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.3.3.2.1.2.1 e1-REQ-4944 Expected Actions

Related to e1-REQ-4940 Discard() Operation Errors and Warnings

Related to e1-REQ-4860 Exception Handling

Related to e1-REQ-4938 Response Message (Full Success Scenario)

The epSOS Consent Service provider shall remove all registry objects and documents as identified in the request. It shall respond to a RemoveObjectsRequest message with a registry response message containing a success indicator.

The epSOS Consent Service provider MUST verify that the requesting service user has sufficient rights to deprecate a consent document for the identified patient. It MUST verify that the consent document was transmitted by the same HP that now wants to discard it.

In case of an error that relates to the transmission of the request or the processing of the epSOS security token, the epSOS Consent Service provider MUST respond with a fault message according to e1-REQ-4860.

3.3.3.2.2 e1-REQ-4945 epSOS Consent Service Protocol Requirements

Related to e1-REQ-1883 epSOS Common Message Format

The epSOS Consent Service operations' request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in e1-REQ-1883.

Port types and bindings MUST be used as defined in the WSDLs given in e1-REQ-4946 (put operation) and e1-REQ-4947 (discard operation). Acc. to this the epSOS Consent Service operations' request and response data MUST be contained within the message body as follows:

epSOS Dispensation Service	Message Body
Put request	ProvideAndRegisterDocumentSet-b_Message (see e1-REQ-4946)
Put response	ProvideAndRegisterDocumentSet-bResponse_Message (see e1-REQ-4946)
Discard request	DeleteMetadata_Message (see e1-REQ-4947)
Discard response	DeleteMetadataResponse_Message (see section e1-REQ-

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4947)

epSOS Consent Service request messages MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in e1-REQ-4884.
epSOS Consent Service response messages MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in e1-REQ-4884.

3.3.3.2.2.1 e1-REQ-4946 IHE XDR Document Recipient WSDL

```
<?xml version="1.0" encoding="utf-8"?>
<definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:ihe="urn:ihe:iti:xds-b:2007"
  xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
  targetNamespace="urn:ihe:iti:xds-b:2007"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" name="DocumentRecipient">
  <documentation>IHE Document Recipient</documentation>
  <types>
    <xsd:schema elementFormDefault="qualified"
      targetNamespace="urn:ihe:iti:xds-b:2007"
      xmlns:ihe="urn:ihe:iti:xds-b:2007">
      <!-- Include the message schema -->
      <xsd:include schemaLocation="../schemas/IHE/XDS.b_DocumentRecipient.xsd"/>
    </xsd:schema>
    <xsd:schema elementFormDefault="qualified"
      targetNamespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
      xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0">
      <!-- Include the message schema -->
      <xsd:include schemaLocation="../schemas/ebRS/rs.xsd"/>
    </xsd:schema>
    <!-- While no elements are directly used from these schema in the WSDL,
        they need to be present here in order for
        code generating toolkits to work properly -->
    <xsd:schema elementFormDefault="qualified"
      targetNamespace="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
      xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0">
      <!-- Include the message schema -->
      <xsd:include schemaLocation="../schemas/ebRS/lcm.xsd"/>
    </xsd:schema>
```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<xsd:schema elementFormDefault="qualified"
  targetNamespace="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
  xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
  <!-- Include the message schema -->
  <xsd:include schemaLocation="../schemas/ebRS/rim.xsd"/>
</xsd:schema>
</types>
<message name="ProvideAndRegisterDocumentSet-b_Message">
  <documentation>Provide and Register Document Set</documentation>
  <part name="body" element="ihe:ProvideAndRegisterDocumentSetRequest"/>
</message>
<message name="ProvideAndRegisterDocumentSet-bResponse_Message">
  <documentation>Provide And Register Document Set Response</documentation>
  <part name="body" element="rs:RegistryResponse"/>
</message>
<binding name="DocumentRecipient_Binding" type="ihe:DocumentRecipient_PortType">
  <soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation name="DocumentRecipient_ProvideAndRegisterDocumentSet-b">
    <soap12:operation soapAction="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"/>
    <input>
      <soap12:body use="literal"/>
    </input>
    <output>
      <soap12:body use="literal"/>
    </output>
  </operation>
</binding>
<service name="DocumentRecipient_Service">
  <port name="DocumentRecipient_Port_Soap12" binding="ihe:DocumentRecipient_Binding">
    <soap12:address location="http://servicelocation/DocumentRecipient_Service"/>
  </port>
</service>
</definitions>

```

3.3.3.2.2.2 e1-REQ-4947 IHE XDS Metadata Update Delete WSDL

```

<?xml version="1.0" encoding="UTF-8"?>
<definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:ihe="urn:ihe:iti:xds-b:2007"
  xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
  xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
xmlns:xdsext="urn:ihe:iti:xds-ebrim:extensions:2010"
targetNamespace="urn:ihe:iti:xds-b:2007"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
name="RespondingGateway_QueryRetrieve">
<documentation>OASIS ebXML Registry Remove Objects operation</documentation>
<types>
    <xsd:schema elementFormDefault="qualified">
        <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
            schemaLocation="../schemas/rs.xsd"/>
        <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
            schemaLocation="../schemas/lcm.xsd"/>
        <xsd:import namespace="urn:ihe:iti:xds-b:2007"
            schemaLocation="../schemas/XDS.b_DocumentRepository.xsd"/>
        <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
            schemaLocation="../schemas/query.xsd"/>
    </xsd:schema>
</types>
<message name="DeleteMetadata_Message">
    <documentation>Delete Metadata</documentation>
    <part name="body" element="lcm:RemoveObjectsRequest"/>
</message>
<message name="DeleteMetadataResponse_Message">
    <documentation>Delete Metadata Response</documentation>
    <part name="body" element="rs:RegistryResponse"/>
</message>
<portType name="DocumentRecipientDeleteMetadata_PortType">
    <operation name="DocumentRecipient_DeleteMetadata">
        <input message="lcm:RemoveObjectsRequest"
            wsaw:Action="urn:ihe:iti:2010:DeleteDocumentSet"/>
        <output message="rs:RegistryResponse"
            wsaw:Action="urn:ihe:iti:2010:DeleteDocumentSetResponse"/>
    </operation>
</portType>
<binding name="DocumentRecipientDeleteMetadata_Binding_Soap12"
    type="ihe:DocumentRecipientDeleteMetadata_PortType">
    <soap12:binding style="document"
        transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="DocumentRecipient_DeleteMetadata">
        <soap12:operation soapAction="urn:ihe:iti:2010:DeleteDocumentSet"/>
        <input>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

        <soap12:body use="literal"/>
    </input>
    <output>
        <soap12:body use="literal"/>
    </output>
</operation>
</binding>
<service name="DocumentRecipientDeleteMetadata_Service">
    <port name="DocumentRecipientDeleteMetadata_Port_Soap12"
        binding="ihe:DocumentRecipientDeleteMetadata_Binding_Soap12">
        <soap12:address
            location="http://servicelocation/DocumentRecipientDeleteMetadata_Service"/>
    </port>
</service>
</definitions>
```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.4 e1-FLD-66 Patient Summary

3.4.1 e1-FLD-76 Conceptual Perspective

3.4.1.1 e1-FLD-123 Information model

3.4.1.1.1 e1-REQ-3873 Minimum common structure of Patient Summary (Basic dataset)

Related to e1-REQ-3892 FR21: Patient Summary Conformance

Related to e1-REQ-4624 Information Model: Patient Summary & ePrescription

The agreed basic dataset is a very fundamental dataset understood as a set of essential information required by the HP to provide safe care to a patient in an unscheduled scenario. The agreed fields MUST be sent even if there is no content available, that is 'null flavor' is allowed (this concept is explained in detail in WP 3.5).

The 'mandatory dataset' is a subgroup of the basic dataset which fields MUST be sent with a valid value, therefore the value MUST NOT be left as 'Null'. It is important to notice that for the 'mandatory dataset', a value of 'Not specified' or a value of 'Not known' can be used only if they are recognized as valid values for that field. (e.g: for 'gender' a value of 'Not Specified' may be used as a valid value by some systems, for example in the United Kingdom system).

The following, is the agreed mandatory dataset:

Identification: ID univocal. "Not specified" value is not allowed

Given Name: "Not specified" value is not allowed

Family name/surname: "Not specified" value is not allowed

Date of birth: must be expressed as a date or just a year. The date must be a valid date. A code should be found for "not known" date (example: 9/9/9999 or 1/1/1900).

Country: "Not specified" value is not allowed

Date of Last Update of PS: It refers to the last version of the PS. It should be a valid date. "Not specified" value is not allowed. It was agreed that it will not be accepted a code for 'not known' date.

Other fields may be included as mandatory as required by some countries to achieve univocal identification of the patient

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.1.1.2 e1-REQ-3874 Maximum common structure of Patient Summary (Extended dataset)

Related to e1-REQ-3892 FR21: Patient Summary Conformance

PATIENT DATA					
VARIABLE (nesting level 1)	VARIABLE S (nesting level 2)	VARIABLES (nesting level 3)	DEFINITION AND COMMENTS	BASIC (Basic)/EXTENDED (Ext) DATASET	MANDATORY Yes/No
Identification	National Health Care patient ID	National Health Care patient ID	Country ID, unique for the patient in that country. Example: ID for United Kingdom patient	Basic	Yes
Personal information	Full Name	Given name	The Name of the patient (Example: John). This field can contain more than one element	Basic	Yes
		Family name/Surname	This field can contain more than one element. Example: Español Smith	Basic	Yes
	Date of Birth	Date of Birth	This field may contain only the year if day and month are not available. Eg:	Basic	Yes

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

 Contact information	Gender	Gender Code	01/01/2009		
			It must contained a recognized valid value for this field	Basic	Pending decision by WP3.6 (in some countries 'gender' is needed for univocal identification of the patient)
	Address	Street	Example: Oxford	Ext	No
		Number of Street	Example: 221	Ext	No
		City	Example: London	Ext	No
		Post Code	Example: W1W 8LG	Ext	No
		State or Province	Example: London	Ext	No
		Country	Example: UK	Ext	No
	Telephone No	Telephone No	Example: +45 20 7025 6161	Ext	No
	E-mail	E-mail	Example: jens@hotmail.co	Ext	No

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

	Preferred HP/Legal organization to contact	m			
		Name of the HP/Legal organization	Name of the HP/name of the legal organization. If it is a HP, the structure of the name will be the same as described in 'Full name' (Given name, family name/surname)	Basic	No
		Telephone No	Example: +45 20 7025 6161	Basic	No
		E-mail	E mail of the HP/legal organization	Basic	No
	Contact Person/legal guardian (if available)	Role of that person	Legal guardian or Contact person	Ext	NO
		Given name	The Name of the Contact Person/guardian (example: Peter. This field can contain more than one element)	Ext	No
		Family name/Surna	This field can contain more	Ext	No

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

		me	than one element. Example: Español Smith		
		Telephone No	Example: +45 20 7025 6161	Ext	No
		E-mail		Ext	No
Insurance information	Insurance Number	Insurance Number	Example: QQ 12 34 56 A	Pending decision by WP3.6 of including it in Basic (in some countries 'Insurance Number' is needed for univocal identification of the patient).	Pending decision by WP3.6 of including it in Basic (in some countries 'Insurance Number' is needed for univocal identification of the patient).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

PATIENT CLINICAL DATA					
VARIABLE (nesting level 1)	VARIABLES (nesting level 2)	VARIABLES (nesting level 3)	COMMENTS	BASIC (Basic)/EXTEN DED (Ext) DATASET	MANDATO RY Yes/No
Alerts	Allergies and intolerances	Allergy description	Description of the clinical manifestation of the allergy reaction. Example: Anaphylactic shock, angioedema (the clinical manifestation also gives information about the severity of the observed reaction)	Basic	No
		Allergy description id code	Normalized identifier	Basic	No
		Onset Date	Date of the observation of the reaction	Ext	No
		Agent	Describes the agent (drug, food, chemical agent, etc) that	Basic	No

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3	
	Version:	1.0
D5.2.3	Date:	31/01/2013

			is responsible for the adverse reaction		
		Agent id code	Normalized identifier	Basic	No
History of past illness	Vaccinations	Vaccinations	Contains each disease against which immunization was given	Ext	No
		Brand name		Ext	No
		Vaccinations id code	Normalized identifier	Ext	No
		Vaccination Date	The date the immunization was received	Ext	No
	List of Resolved, Closed or Inactive problems	Problem Description	Problems or diagnosis not included under the definition of 'Current problems or diagnosis'. Example: hepatic cyst (the patient has been treated with an hepatic cystectomy that solved the problem and	Ext	No

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

		therefore it's a closed problem)		
	Problem Id (code)	Normalized identifier	Ext	No
	On set time	Date of problem onset	Ext	No
	End date	Problem resolution date	Ext	No
	Resolution Circumstances	Describes the reason by which the problem changed the status from current to inactive (e.g. surgical procedure, medical treatment, etc). This field includes 'free text' if the resolution circumstances are not already included in other fields. Example: It can happen that this field is already included in other like	Ext	No

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

			Surgical Procedure, medical device etc, eg: hepatic cystectomy (this will be the 'Resolution Circumstances' for the problem 'hepatic cyst' and will be included in surgical procedures)		
Surgical Procedures prior to the past six months		Procedure description	Describes the type of procedure	Ext	No
		Procedure Id (code)	Normalized identifier	Ext	No
		Procedure date	Date when procedure was performed	Ext	No
Medical problems	List of Current Problems/Diagnosis.	Problem/diagnosis description	Problems/diagnosis that fit under these conditions: conditions that may have a chronic or relapsing course (eg: exacerbations of asthma, irritable bowel syndrome),	Basic	No

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

			conditions for which the patient receives repeat medications (eg: diabetes mellitus, hypertension) and conditions that are persistent and serious contraindications for classes of medication (eg: dyspepsia, migraine and asthma)		
			Problem Id (code)	Normalized identifier	Basic No
			Onset time	Date of problem onset	Basic No
			Medical Devices and implants	Device and implant Description	Describes the patient's implanted and external medical devices and equipment that their health status depends on. Includes devices as cardiac pacemakers, implantable Basic No

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3	
	Version:	1.0
D5.2.3	Date:	31/01/2013

Major Surgical Procedures in the past 6 months			defibrillator, prothesis, ferromagnetic bone implants etc that are important to know by the HP		
	Device Id code	Normalized identifier	Basic	No	
	Implant date		Basic	No	
	Procedure description	Describes the type of procedure	Basic	No	
	Procedure Id (code)	Normalized identifier	Basic	No	
	Procedure date	Date when procedure was performed	Basic	No	
	Treatment Recommendations	Recommendations Description	Therapeutic recommendations that do not include drugs (diet, physical exercise constraints, etc.)	Ext	No
	Recommendation Id (code)	Normalized identifier	Ext	No	

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

	Autonomy/Invalidity	Description	Need of the patient to be continuously assisted by third parties. Invalidity status may influence decisions about how to administer treatments	Ext	No
		Invalidity Id code	Normalized invalidity ID (if any, otherwise free text)	Ext	No
Medication Summary	List of current medicines. (All prescribed medicine whose period of time indicated for the treatment has not yet expired whether it has been dispensed or not.)	Active ingredient	Substance that alone or in combination with one or more other ingredients produces the intended activity of a medicinal product. Example: Paracetamol	Basic	No
		Active ingredient id code	Code that identifies the Active ingredient	Basic	No
		Strength	The content of the active ingredient	Basic	No

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

		expressed quantitatively per dosage unit, per unit of volume or per unit of weight, according to the pharmaceutical dose form. Example: 500 mg per tablet		
	Pharmaceutical dose form	It is the form in which a pharmaceutical product is presented in the medicinal product package (e.g. tablets, syrup)	Ext	No
	Number of units per intake	The number of units per intake that the patient is taking. Example: 1 tablet	Basic	No
	Frequency of intakes	Frequency of intakes (per hours/day/month/ week...). Example: each 24 hours	Basic	No
	Duration of treatment	Example: during 14 days	Basic	No

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

		Date of onset of treatment	Date when patient needs to start taking the medicine prescribed	Basic	No
Social History	Social History Observations	Social History Observations related to: smoke, alcohol and diet.	Example: cigarette smoker, alcohol consumption...	Ext	No
		Reference date range	Example: from 1974 thru 2004	Ext	No
Pregnancy History	Expected date of delivery	Expected date of delivery	Date in which the woman is due to give birth. Year, day and month are required. Eg: 01/01/2010	Ext	No
Physical findings	Vital Signs Observations	Blood pressure	One value of blood pressure which includes: systolic Blood Pressure and Diastolic Blood pressure	Ext	No
		Date when blood pressure was measured	Date when blood pressure was measured	Ext	No

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Diagnostic tests	Blood group	Result of blood group	Result from the blood group test made to the patient	Ext	No
		Date	Date in which the blood group test was done. This field may contain only the year if day and month are not available. Eg: 01/01/2009	Ext	No

{C}

PATIENT SUMMARY DATA (Information about the PS itself)					
VARIABLE (nesting level 1)	VARIABLE S (nesting level 2)	VARIABLE S (nesting level 3)	COMMENTS	BASIC (Basic)/EXTENDED (Ext) DATASET	MANDATORY Yes/No
Country	Country	Country	Name of country A	Basic	Yes
Patient Summary	Date Created	Date Created	Data on which PS was generated	Basic	No

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

	Date of Last Update	Date of Last Update	Data on which PS was updated (data of last version)	Basic	Yes
Author/Nature of the patient summary	Author of the patient summary	Author of the patient summary	To highlight if the data is collected manually by an HP or is collected automatically from different sources (eg: hospital doctor repository, GPs...etc) through predetermined clinical rules.	Basic	No
Legal entity	Responsible of the PS data	Responsible of the PS data	At least an author organization (HPO) shall be listed. In case there is not HPO identified at least a HP shall be listed	Basic	No

Patient Summary data set

The field "alerts" was originally defined to include all the important and objective medical

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

information that should be highlighted (such as allergies, thrombosis risk, immune deficit ...etc). When defining the content only allergies and intolerance to drugs appear to be the common understanding and the easiest to be transferred.

A lot of surveys are being made in different countries (not only in Europe) to make a more evidence-based definition of what should be inside and what shouldn't in the concept "alerts" so, for at that first step, not enough information could be provided to take a further decision. On the other hand some people proposed that it could be considered more a way to present the information than a different field.

The final decision was to keep allergies and intolerance as the content of that field in that first step and to get the subject retaken in epSOS2 for a more complete solution if possible. The feeling was that the concept of alerts is a positive one to be defined in a PS but that no further content could be describe at this moment.

3.4.1.1.3 e1-REQ-5142 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-1669 About HP Prescriber Identification in the ePrescription

Variable	Definitions	MS: Minimum Max: maximum	Comments	Example
Given Name	The Name of the Prescriber	MS	This field can contain more than one element	Marta
Family name/surname	The surname/s of the Prescriber	MS	This field can contain more than one element	Español Smith
HP Id number	The identification of the person as HP	MS		12345

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Profession		MS		Physician
Specialist		Max		Dermatologist
Prescriber Facility Address:	The place (complete address) where the prescriber made the prescription		This is not a field but a block of information made up of the following fields. This might not be in the dataset but this information needs to be available for the process traceability (FR20)	e.g., Los Bermejales Health Care Centre. Alemania St. Seville, 41018. Spain
Name of the Facility		Max		For instance, the name of the building: Los Bermejales
Street Address		Max		Alemania Street
City		Max		Seville
State or Province		Max		Seville
Zip or Postal Code		Max		41018
Telephone		Max		+34 954123123
Contact email of the centre or of the prescriber		Max		losbermejaleshealthcentre@xxx.es
Country	The country where the prescription	MS	The dispenser needs to know the country	Spain

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

	was made		where he is consulting the information from	
Prescriber Organization:			<p>This is not a field but a block of information made up of the following fields.</p> <p>This might not be in the dataset but this information needs to be available for the process traceability (FR20)</p>	
Organization Name		Max		e.g. Andalusia Health Service
Organization Identifier		Max	This field can be numbers and/or letters	123458xfs

3.4.1.2 e1-FLD-124 Computational Dimension

3.4.1.2.1 e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Related to e1-REQ-3867 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-3888 Data Integrity

Related to e1-REQ-4411 Data Origin and Data Authenticity

Related to e1-REQ-3861 FR19: Patient Summary of Country A available

Related to e1-REQ-4672 FR20: Information Traceability

Related to e1-REQ-3892 FR21: Patient Summary Conformance

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Related to e1-REQ-3893 FR22: Uniqueness of Patient Summary

Related to e1-REQ-3863 HP-B Identification and Authentication

Related to e1-REQ-3869 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-3876 NFR01- Service availability

Related to e1-REQ-3878 NFR03- Response time

Related to e1-REQ-3880 NFR05- Access control

Related to e1-REQ-4564 NFR09- Trust between countries

Related to e1-REQ-3885 NFR10- Guaranteed delivery

Related to e1-REQ-3886 NFR11- Single session

Related to e1-REQ-3887 NFR12- Supervision services

Related to e1-REQ-3868 Patient Identification

Related to e1-REQ-4599 REQ 3.3.14 Medication Summary only accessible as part of Patient Summary

Related to e1-REQ-3871 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-3865 Structured Information and Semantic Compliance

Related to e1-REQ-3872 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-3889 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-3866 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-4623 epSOS PatientService Service Interface & Functional Specification

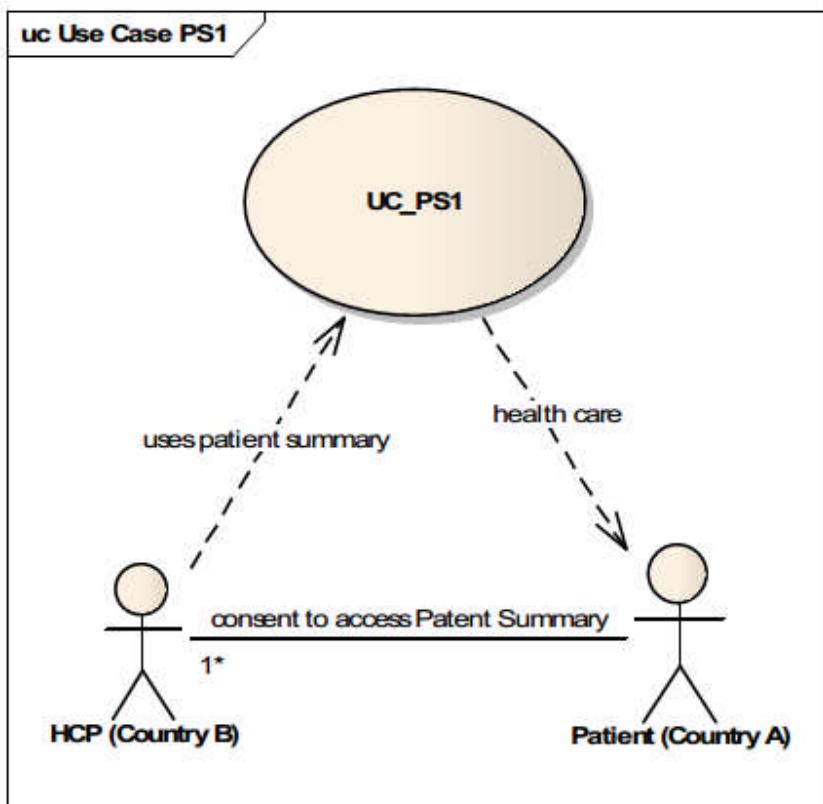
The Patient Summary might be used in two distinct use cases.

From a technical point of view the difference is merely that in use case 1 the HP does not have any records of the patient, in use case 2 there might be a record from previous visits or previous data exchange. It must be however noted that the two cases are very different in terms of regulations that are relevant to cross border care.

Patient Summary Use Case 1:

When a person is an occasional visitor in country B, for example on holiday or business. In such cases the visit is irregular, infrequent and may often not be repeated. The HP has no records from previous encounters.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



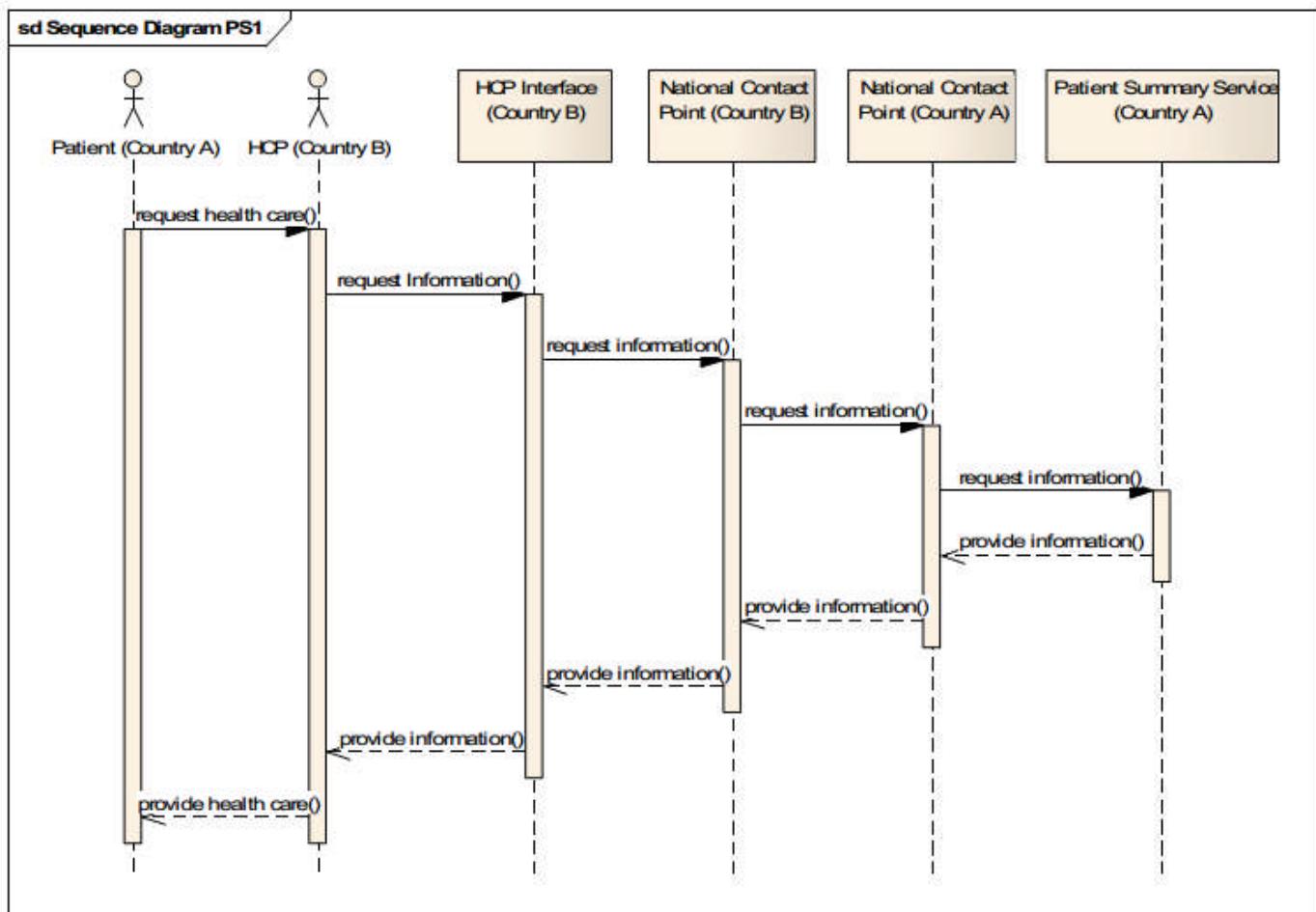
Use Case Patient Summary “occasional visitor”

In the use case the following entities participate:

- A patient from country A in need of health care in country B.
- A Health Professional (HP) in country B.
- A HP interface in country B which serves as a communication interface to a National Contact Point (NCP) of country B.
- A NCP in country B receiving a request from HP interface (e.g. embedded in the national IT infrastructure of country B) and connecting to the NCP of country A.
- A NCP in country A communicating with the existing national infrastructure of country A (where information about the patients summary are provided) and the NCP in country B.
- A Patient Summary (PS) Service in country A providing information for the NCP in country A.

More detailed the use cases may be illustrated in this way:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



Sequence Diagram Patient Summary “occasional visitor”

The above diagrams contain the main steps:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Step	Name	Description	Output	Entities
1	Trigger for health care	A patient from country A requests or is in need of health care and contacts an HCP in country B.	Trigger to HCP	Patient, HCP
2	Request for information from Patient Summary	During consultation with the patient the HCP generates and sends a request to the NCP B using his/her HCP interface (depends on if the visit is regular or occasional!)	Request to NCP B	HCP, HCP interface, NCP B
3	NCP transfer 1	NCP B transfers the request to NCP A which transfers it to the PS Service for response	Information transfer to PS Service	NCP A, NCP B, PS Service
4	NCP transfer 2	NCP A receives an response from PS Service and transfers it to NCP B	Information transfer from PS Service	NCP A, NCP B, PS Service
5	Response from Patient Summary	The NCP B transfers the response to the HCP interface.	Response to the HCP interface	NCP B, HCP interface
6	HCP uses information from Patient Summary and provides health care to the patient	The HCP finishes the consultation using the retrieved information provided in the HCP interface.	Patient receives health care with the help of information from Patient Summary	HCP, HCP interface, patient

Use Case description Patient Summary

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.2 e1-FLD-77 Logical Perspective

3.4.2.1 e1-REQ-3863 HP-B Identification and Authentication

Synchronized with e1-REQ-1981 HP-B Identification and Authentication

Tested by e1-REQ-5147 HP-B Identification and Authentication

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

The identity and authenticity of an HP MUST be verified before he can use epSOS cross-border services. Each data access request MUST contain sufficient and verifiable information about (the identity and the role of) the accessory for assessing a country-A national security policy.

3.4.2.1.1 e1-TXT-586 Note

Associated Goals:

To provide security to the process.

To ensure that the HP is legally allowed to perform the functionalities described in this document.

Prevention of disclosure to unauthorized persons.

Actors: HP-B, NCP-B

3.4.2.2 e1-REQ-3869 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-2206 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Tested by e1-REQ-5148 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

epSOS agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations must be secured and codes of conduct as part of the epSOS Information Governance must be elaborated.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.4.2.2.1 e1-TXT-459 Note

Associated Goals:

To avoid having to identify all professionals and institutions from a foreign country in the country of origin. On the one hand, each HP will be unequivocally identified and authenticated in his local system and must be identified based on his/her role/profile. On the other hand, Health Care Provider Organisation provides HP a status, a function, an authentication from which the HP trust is derived. Furthermore, Health Authorities Institutions assign and assure the status, the role, and sometimes the authentication of HP.

Actors: HP-B with rights for accessing PS, NCP-A, NCP-B

3.4.2.3 e1-REQ-3868 Patient Identification

Synchronized with e1-REQ-1973 Patient Identification

Tested by e1-REQ-5149 Patient Identification

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

The intended recipient of medical data MUST identify the patient with sufficient accuracy. Medical data MUST only be disclosed after the patient was identified with sufficient accuracy.

Technical means for patient identification MUST NOT use or disclose medical data about this patient. Patient identifiers SHOULD NOT technically enable any unlawful linkage of the patient's medical data to other sanctioned personal data beyond any legitimate purpose from other domains. If technical means for identity protection (e.g. pseudonymization) are used, these MUST NOT disqualify the responsible parties to lawfully provide the patient access to his/her data. The original identification of the patient MUST NOT rely on the existence of electronic identifiers (eIDs). epSOS use cases MAY define further constraints on the accuracy and means of patient identification for that specific use case (e.g. identification by name considered as insufficient for the 112 use case).

3.4.2.3.1 e1-TXT-460 Note

Associated Goals:

To have certainty of the identity of the patient

Actors: HP-B with rights for accessing PS, NCP-A, NCP-B

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.4.2.4 e1-REQ-3889 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-1977 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Tested by e1-REQ-5166 Willful Disclosure (Data Confidentiality)

Medical data MUST NOT be disclosed to persons or organization unless they have been authorized by the patient (see »Consent-2; PIN«) and the disclosure is legally or explicitly required for fulfilling the treatment.

Medical data MUST NOT be disclosed to others than healthcare professionals or healthcare professional organizations in any case.

Medical data MUST NOT be transferred to other destinations unless this disclosure has been authorized by the patient or is mandated by national law.

The proper enforcement of the willful disclosure acc. to »consent-2« MUST be controllable and verifiable by the patient.

Implications:

Data MUST be encrypted during transfer and whenever it is stored at (intermediate) nodes outside the trusted environment of an HP (see “IT-Systems directly controlled by HPs”).

Depending on how “controllable” and “verifiable” are defined this requirement as well implies a need for secure end-to-end encryption between trusted HP environments.

3.4.2.4.1 e1-TXT-470 Note

Associated Goals:

Manifesting the legal foundation for a lawful data processing

Protecting and safe-guarding the patients medical information

Ensuring the involved HP to be fully compliant with their professional code

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.4.2.5 e1-REQ-3866 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Tested by e1-REQ-5150 Willful Provisioning of Data (»Consent-1«)

The provisioning of medical data for cross-border medical use cases MUST require a willful and documentable act of agreeing by the patient.

This willful act MUST fulfill all requirements of an informed, free consent acc. to country-A legislation. It MUST deliver an appropriate level of data security and privacy for the patient as it is defined in his home country.

This willful act MUST be designed in full anticipation of a cross-border health data exchange scenario.

The respective consent MUST be given in written form and MUST be signed by the patient. A qualified digital signature MAY be used instead of a wet signature.

A country MUST assure that patient data is only accessible if a valid patient consent for data provisioning exists. A country MUST ensure that data is no longer accessible after the respective consent has been revoked or expired.

A HP- B is not required to explicitly verify the existence of a patient's »consent-1« (that was formerly given in country-A) as it is assumed that all epSOS country-A have established secure processes for enforcing the revocation of consents and therefore will not provide data to a country-B unless a valid »consent-1« exists.

3.4.2.6 e1-REQ-3867 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

Tested by e1-REQ-5170 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Triggering a cross-country transfer of medical data MUST require a willful act by the patient.

This willful act MUST express the patient's explicit authorization to allow an identifiable healthcare professional the execution of defined data access operations.

This willful act MUST express the explicit authorization of the patient to transfer medical data to the formerly identified and specifically documented destination.

Countries MAY require that this willful act is documented by an explicit, written and informed consent that is to be signed by the patient.

Implications:

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

The authorization to perform a specific operation can only be given and documented in country-B (as this authorization requires the identification of both the patient and the HP-B).

Therefore epSOS MUST provide technical means to transmit information about the authorization/PIN to country-A before or while a data access operation is triggered.

3.4.2.6.1 e1-TXT-461 Note

Associated Goals:

Manifesting the legal foundation for a lawful data processing.

Granting the patient his specific rights according to data protection regulations.

Deciding on whether a certain request for data is legitimated by the consent or not.

Actors: HP-B, NCP-A, NCP-B

This requirement is subject to legal aspects defined in WP2.1 'Analysis of legal and regulatory issues' and the different solutions to handle it are described in WP3.6 'Identity Management'.

3.4.2.7 e1-REQ-3865 Structured Information and Semantic Compliance

Synchronized with e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Tested by e1-REQ-5151 Structured Information and Semantic Compliance

epSOS MUST define the structure and semantics of all document types which are required to be shared cross-border within epSOS use cases (pivot schema and common terminologies).

It is the responsibility of each PN to preserve the semantics of original data when this is transformed and transcoded into the common epSOS format as defined for the respective document type. Transformation services within a country and epSOS semantic services should guarantee the smoothest semantic transformation, keeping the meaning and the value of the source document, considering the liability for the transformation, and assuring the reproducibility of the semantic transformation.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.2.7.1 e1-TXT-462 Note

Associated Goals:

Safety reason.

HP understands the meaning of all the fields that are going to be shown to him.

To provide the HP with the necessary information to deliver safe care to the patient.

To guarantee the safety of the patient through a proper understanding of the received information.

To ensure safety delivery of care to patients thanks to the faithful exchange of meanings between systems and between systems and people.

To reduce time in searching necessary information to provide Health Care to the patient.

To facilitate the later treatment of the information to assure its comprehension through semantic tools, systems of codification or of translation according to how it will be established later in the epSOS LSP project.

Actors: HP-B, NCP-A, NCP-B

3.4.2.8 e1-REQ-3871 Semantic Interoperability of Structured Clinical Content

Synchronized with e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Tested by e1-REQ-5152 Semantic Interoperability of Structured Clinical Content

Medical information shared among countries MUST be understandable (in the correct context) for the receiver. HP-B MUST be enabled to view and/or process medical documents encoded in a way that best matches the document structure and clinical terms that are commonly used in country-B.

Implications:

epSOS MUST provide semantic services that allow for translation/mapping of clinical terms.
epSOS SHOULD use a common pivot schema and terminology set in order to limit the number of mappings that have to be defined and maintained.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.2.8.1 e1-TXT-464 Note

Associated Goals:

Safety reasons.

HP understands the meaning of all the fields that are going to be shown to him.

To provide the HP with the necessary information to deliver safe care to the patient.

To guarantee the safety of the patient through a proper understanding of the received information.

To ensure safety delivery of care to patients thanks to the faithful exchange of meanings between systems and between systems and people.

Actors: HP-B with rights for accessing PS, NCP-A, NCP-B

3.4.2.9 e1-REQ-3861 FR19: Patient Summary of Country A available

Tested by e1-REQ-5154 FR19: Patient Summary of Country A available

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

In order for the HP-B to be able to access the PS of a patient, the country A MUST have that PS available.

3.4.2.9.1 e1-TXT-465 Note

Associated Goals:

PS of country A must be available to be requested by HP of any other country. After the identification of the patient who requests Health Care in country B, HP-B requests the visualization of the PS the patient has in country A.

Actors: HP-B with rights for accessing PS, NCP-A, NCP-B

3.4.2.10 e1-REQ-5131 Minimum and Maximum Data Sets

Synchronized with e1-REQ-1986 Minimum and Maximum Data Sets

Tested by e1-REQ-5153 Minimum and Maximum Data Sets

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Every PN MUST provide means that enable an HP IT-System to properly translate, display and process mandatory data entries within epSOS documents. Every PN SHOULD provide means that enable an HP IT-System to properly translate, display and process optional data entries within epSOS documents.

PN MAY define additional data entries within epSOS documents as long as this does not violate the defined pivot schema. PN that receive such extended documents MAY ignore all data elements not defined by epSOS.

3.4.2.11 e1-REQ-5133 Peering Original Document

Synchronized with e1-REQ-1988 Peering Original Document

Tested by e1-REQ-5174 Peering Original Document

Whenever original data is transcoded/translated for the purpose of cross-border document sharing, the receiver of that data MUST be enabled by epSOS to view that data without transcoding/translation, too. epSOS use case specifications MAY define default behaviors and constraints for peering original documents.

3.4.2.12 e1-REQ-3872 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Tested by e1-REQ-5163 Traceability and Exercise of Patient Information Rights

Cross-border exchange of medical data MUST be documented in a fully traceable, reconstructable, and seamless fashion.

Cross-border exchange of medical data MUST produce a usable chain of digital evidence that enables both, the patient and his assigned DPA, to pursue, enforce, and proof any assumed or detected violation of the patient's data protection and privacy rights.

The chain of digital evidence MUST disclose the minimum of personal health data required to serve its purpose and MUST be specifically safeguarded against wrongdoing. Part of these safeguards MUST be a protocol that is not accessible to HPs.

Implications:

Audit trails SHOULD be written at both NCPs. For the purpose of data minimization NCP audit trails SHOULD not include medical data but just refer to (and safeguard) respective audit trails within HP systems.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.2.12.1 e1-REQ-4672 FR20: Information Traceability

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

The information describing the process and the data involved in the process must be able to be traced and recovered. This includes all the information that has been considered as basic and extended data in the PS. It also includes such information as the location and the identification of the requester , time of consulting and the rest of the information contained within the PS effectively accessed and transferred to the HP-B.

3.4.2.12.2 e1-TXT-466 Note

Associated Goals:

Security reasons.

Legal reasons.

Enabling a transparent and 'able to be reconstructed' system operation

Documenting compliance and legitimacy of data accesses

Making the epSOS LSP services auditable

Actors: HP-B with rights for accessing PS, NCP-A, NCP-B

3.4.2.13 e1-REQ-3892 FR21: Patient Summary Conformance

Tested by e1-REQ-5201 FR21: Patient Summary Conformance

Related to e1-REQ-3874 Maximum common structure of Patient Summary (Extended dataset)

Related to e1-REQ-3873 Minimum common structure of Patient Summary (Basic dataset)

Related to e1-REQ-2094 Patient Summary template conformance

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

The structure of the patient summary is an agreed structure; the fields to be shared MUST be the one agreed in both the basic and extended summary, no less and no more information can be shared through the Patient Summary document.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.4.2.14 e1-REQ-3893 FR22: Uniqueness of Patient Summary

Tested by e1-REQ-5202 FR22: Uniqueness of Patient Summary

Related to e1-REQ-4624 Information Model: Patient Summary & ePrescription

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Only one PS must be exchanged by each patient.

3.4.2.15 e1-REQ-4599 REQ 3.3.14 Medication Summary only accessible as part of Patient Summary

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Tested by e1-REQ-5203 REQ 3.3.14 Medication Summary only accessible as part of Patient Summary

Medication Summary must not be supposed to be accessible as a sole data object (as part of the Patient Summary). Transactions shall not cover the retrieval operation to get only the medication summary.

3.4.2.16 e1-REQ-3876 NFR01- Service availability

Related to e1-REQ-4895 Expected Actions

Tested by e1-REQ-5169 NFR01 - Service availability

Synchronized with e1-REQ-4557 NFR01- Service availability

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Each unpredictable service interruption MUST be detected as soon as possible. The origin of the failure (HP system, NCP system...) MUST be explained. It MUST be declared which systems or types of information that cannot be reached at the present time due to circumstances or technical failures. The procedure to follow MUST be specified in order to come back to a normal mode.

Instead of completely unavailability, the service MAY be degraded. This state MUST be defined and when this happens, the suitable alerts and the procedures to follow MUST be defined.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.2.16.1 e1-TXT-467 Note

Associated Goals:

The epSOS service will be continuously available

3.4.2.17 e1-REQ-3888 Data Integrity

Synchronized with e1-REQ-1978 Data Integrity

Tested by e1-REQ-5164 Data Integrity

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

The integrity of transmitted data MUST be preserved when information is transmitted between different entities (legally or technically defined). It must be verifiable to a data receiver that data has not been damaged, altered or (partially) lost.

3.4.2.17.1 e1-TXT-468 Note

Associated Goals:

To have secure communication means between National Contact Points

3.4.2.18 e1-REQ-3878 NFR03- Response time

Tested by e1-REQ-5165 NFR03 - Response time

Synchronized with e1-REQ-4559 NFR03- Response time

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

The system MUST be able to answer to the HP in an acceptable response time.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.4.2.18.1 e1-TXT-469 Note

Associated Goals:

Information has to travel from one country to another. An acceptable time response not only applies to the receipt of information, but also to the identification and authentication of HP and patient

The system should provide an acceptable end-to-end response time, not degrading or delaying the already existing services because the patient is waiting while the system accesses and shows the required information

The access times should be tested continually by the system to give the user some idea of what to expect

3.4.2.19 e1-REQ-3880 NFR05- Access control

Tested by e1-REQ-5167 NFR05 - Access control

Synchronized with e1-REQ-4561 NFR05- Access control

Synchronized with e1-REQ-5110 NFR05- Access control

Synchronized with e1-REQ-5111 NFR05- Access control

Synchronized with e1-REQ-5123 NFR05- Access control

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

As authorisations involve the existence of a treatment context inside a HCPO, these treatment relationships must be justifiable on demand. The communication partners (origin, destination, and potential facilitators) MUST be known to each other with prior positive verification that all involved partners are authentic (security features to be provided by the means of an identity (subjects, actors, objects) and access management).

3.4.2.19.1 e1-TXT-471 Note

Associated Goals:

For traceability reasons

For security reasons

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

To assure confidentiality

For Confidentiality and integrity of medical data reasons

To align to the European Data Protection Regulations

3.4.2.20 e1-REQ-4411 Data Origin and Data Authenticity

Synchronized with e1-REQ-1984 Data Origin and Data Authenticity

Tested by e1-REQ-5168 Data Origin and Data Authenticity

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

The intended recipient of a medical data communication MUST be able to determine the originator and level of authenticity of the medical data received. Information on the identity and authenticity of the data originator that is assigned to the data or its metadata MUST NOT be altered during cross-border transfer.

3.4.2.20.1 e1-TXT-474 Note

Associated Goals:

To guarantee that the issuer of the information exchanged cannot refuse that the issuance has taken place

3.4.2.21 e1-REQ-4564 NFR09- Trust between countries

Related to e1-REQ-2206 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Tested by e1-REQ-5175 NFR09 - Trust between countries

Synchronized with e1-REQ-4565 NFR09- Trust between countries

Synchronized with e1-REQ-5095 NFR09- Trust between countries

Synchronized with e1-REQ-5096 NFR09- Trust between countries

Synchronized with e1-REQ-5114 NFR09- Trust between countries

Synchronized with e1-REQ-5122 NFR09- Trust between countries

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Related to e1-REQ-4591 REQ 3.3.6 Secure Context Establishment

All the countries involved in the project are integrated into one circle of trust (technical). An agreed framework for creating trust MUST be established, encompassing processes and procedures for critical data protection, privacy and confidentiality issues as well as mechanisms for their audit. Such issues include, but are not limited to:

- Identification, authentication and authorisation mechanisms
- Security and trust mechanisms
- Recording and exchanging patient consent

3.4.2.21.1 e1-TXT-650 Note

Associated Goals:

To enable the exchange of information between countries.

To avoid having to identify all professionals and institutions from a foreign country in the country of origin. On the one hand, each HP will be unequivocally identified and authenticated in his local system and must be identified based on his/her role/profile. On the other hand, Health Care Provider Organisation provides HP a status, a function, an authentication from which the HP trust is derived. Furthermore, Health Authorities Institutions assign and assure the status, the role, and sometimes the authentication of HP .

3.4.2.22 e1-REQ-3885 NFR10- Guaranteed delivery

Related to e1-REQ-4895 Expected Actions

Tested by e1-REQ-5171 NFR10 - Guaranteed delivery

Synchronized with e1-REQ-4566 NFR10- Guaranteed delivery

Synchronized with e1-REQ-5115 NFR10- Guaranteed delivery

Synchronized with e1-REQ-5116 NFR10- Guaranteed delivery

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

When information is sent from one country to another, it MUST be assured that the information has been properly received by the user in the receiver country.

3.4.2.22.1 e1-TXT-475 Note

Associated Goals:

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

security reasons

to check that the ePrescription service has been properly completed

3.4.2.23 e1-REQ-3886 NFR11- Single session

Tested by e1-REQ-5172 NFR11 - Single session

Synchronized with e1-REQ-4567 NFR11- Single session

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

In order to avoid fraud, it MUST NOT possible to open more than one session for the patient at a time.

3.4.2.23.1 e1-TXT-476 Note

Associated Goals:

For security reasons

To avoid a patient withdrawing the same medicine at the exact time from different pharmacies

3.4.2.24 e1-REQ-3887 NFR12- Supervision services

Tested by e1-REQ-5173 NFR12 - Supervision services

Synchronized with e1-REQ-4568 NFR12- Supervision services

Synchronized with e1-REQ-5117 NFR12- Supervision services

Synchronized with e1-REQ-5130 NFR12- Supervision services

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

A service MUST be put in place to detect all the technical exceptions and to check and monitor the performance of the service (time response, communications...).

3.4.2.24.1 e1-TXT-477 Note

Associated Goals:

To assure the availability and to avoid degradation of the service

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.4.2.25 e1-FLD-126 Information Model

3.4.2.25.1 e1-REQ-4624 Information Model: Patient Summary & ePrescription

Related to e1-REQ-3893 FR22: Uniqueness of Patient Summary

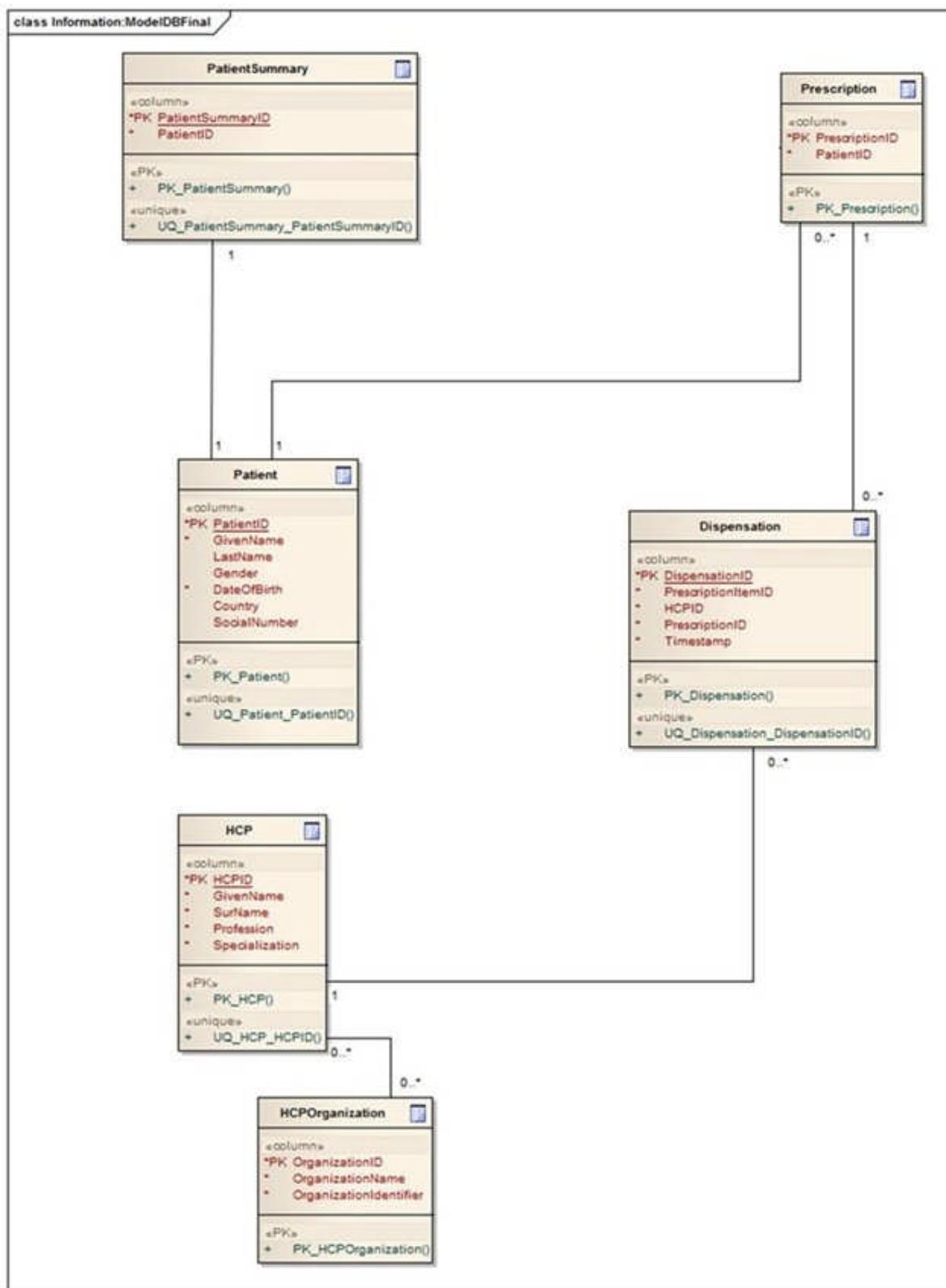
Related to e1-REQ-3873 Minimum common structure of Patient Summary (Basic dataset)

Synchronized with e1-REQ-4626 Information Model: Patient Summary & ePrescription

Synchronized with e1-REQ-4633 Information Model: Patient Summary & ePrescription

Related to e1-REQ-2094 Patient Summary template conformance

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
D5.2.3	Version:	1.0
	Date:	31/01/2013



	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Health Professional (HP)

A health care professional is a physician participating in epSOS identifiable by its unique id. It is affiliated to zero or more health care professional organizations, depending on national legislation.

The HP contains information as defined in D3.1.2. A HP is related to 0..n HCPOs and is associated with 1..n Healthcare Professional Addresses.

Health Care Professional Organization (HCPO)

A Health Care Professional Organization is a logical entity within the national environment known to the NCP and uniquely identifiable by its id.

The HCPO object contains information defined in D3.1.2. An HCPO is related to 1..n HPs. At any given time in the context of an epSOS transaction, an HP is associated with only one HCPO.

Patient

A patient is an individual person participating in epSOS by giving permission (prior consent) in his home community to process his/her medical data to a foreign participating nation.

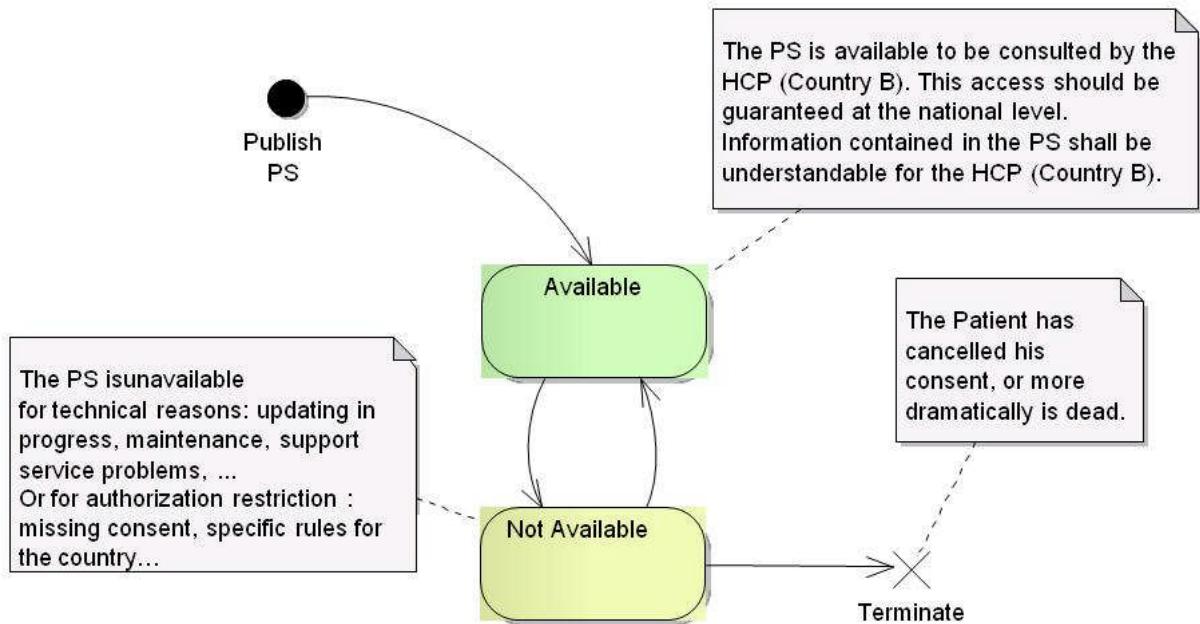
The Patient object contains information defined in D3.1.2. A patient is related to 1..1 PS, 0..* ePs and 0..* eDispenses.

3.4.2.25.2 e1-REQ-4625 State Model: Patient Summary

The patient summary contains the patient's medical information. The patient summary may also include the medication summary. As previously stated every access to the patient summary and ePrescription data is read only . There will be no write access to this data within epSOS. Figure 28 shows the lifecycle of a PS within epSOS. The PS is available if the patient has agreed to take part in epSOS, and is not available if the patient decides not to take part in epSOS

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

anymore.



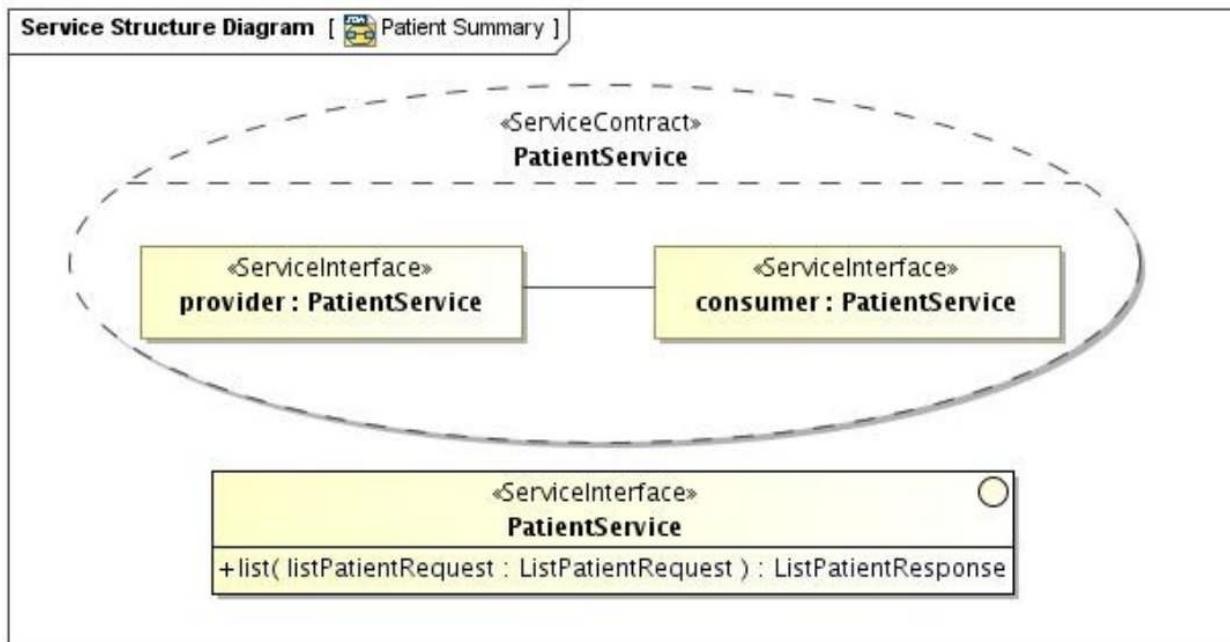
3.4.2.26 e1-FLD-125 Computational Dimension

3.4.2.26.1 e1-REQ-4623 epSOS PatientService Service Interface & Functional Specification

Related to e1-REQ-4410 Patient Summary Use Case “Occasional Visitor” visit to Health Care Professional in country B

Related to e1-REQ-4840 epSOS PatientService Service Interface & Functional Specification

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



Operation list()

Description Obtain the patient summary of the identified patient

Requestor Consuming Gateway at NCP-B

Input
Message

Body Identifier of the patient whose patient summary is requested
Optional: epSOS CDA template qualifier (pivot and/or source coded document)

Security Token X.509 Gateway Certificate

epSOS HCP Identity Assertion
epSOS Treatment Relationship Confirmation Assertion (opt.)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Output Message in successful Case	ListPatientResponse
	<hr/>
Body	epSOS-encoded patient summary (CDA) or/and source coded patient summary (PDF) of the identified patient
	<hr/>
Security Token	X.509 Gateway Certificate
	<hr/>
Precondition of success scenario	<p>The requestor is able to locate the service provider</p> <p>The certificate of the NCP-A gateway is available to the requestor.</p> <p>The requestor is able to verify the certificate of the NCP-A gateway.</p> <p>The NCP-A gateway is able to verify the requestor's certificate.</p> <p>An HCP identity assertion has been issued by NCP-A and is available to the requestor</p> <p>The NCP-A gateway is able to verify the validity of the HCP identity assertion</p> <p>NCP-A and NCP-B agreed on a common ID for referencing to the patient</p> <p>An TRC assertion has been issued by NCP-B and is available to the requestor</p> <p>The NCP-A gateway is able to verify the validity of the TRC assertion</p>
	<hr/>
Main success scenario	<p>Actions of the epSOS Patient Service provider:</p> <p>validate the message signature</p> <p>verify HCP identity assertion and TRC assertion</p> <p>extract the patient ID from the message body</p> <p>verify that the patient has given consent to epSOS and that the consent is valid</p> <p>retrieve patient's patient summary source document</p> <p>enforce national security policy and (if available) patient privacy policy</p>

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

- verify authenticity and integrity of the patient summary
- transform patient summary into epSOS pivot format (if requested and needed)
- render PDF from source document (if requested and needed)
- sign the response message and send it to the requestor

Fault	Preconditions for a success scenario are not given
	Requestor has insufficient rights to access the patient's medical summary
	No patient summary is available for the identified patient
	The patient summary cannot be provided in the requested encoding
	Temporary failure (e. g. authenticity verification cannot be performed due to a PKI failure)
Warning	Country A allows for data hiding; a respective disclaimer SHOULD be shown to the HP
	The HP MUST additionally consider the source coded document because this MAY contain additional information
	Not all sections of the patient summary are provided Partial Delivery: It must be assessed if partial delivery conditions could be signaled on the content level (within the documents) instead of transmitting such information on the transaction level.
	The computation of the CDA encoded patient summary was not approved by an HP; a respective disclaimer MUST be shown to the HP

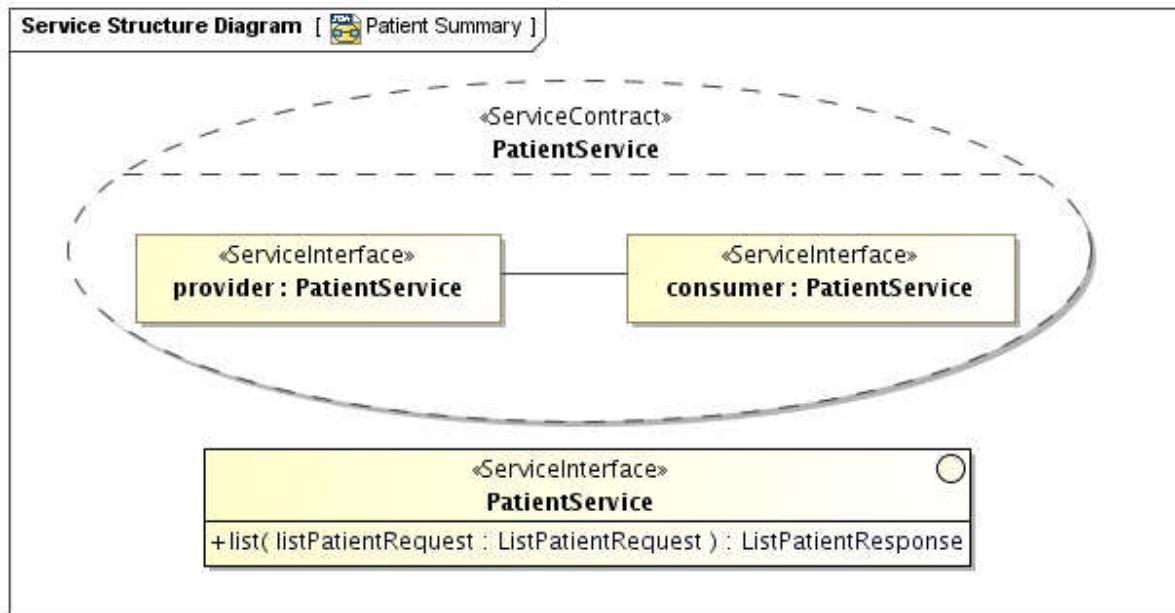
3.4.2.26.2 e1-REQ-4840 epSOS PatientService Service Interface & Functional Specification

Related to e1-REQ-4623 epSOS PatientService Service Interface & Functional Specification

Related to e1-REQ-4841 General Considerations for Successful Service Operations

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Related to e1-REQ-4886 epSOS Patient Service Message Specification



Operation: list

Operation list()

Description Obtain the patient summary of the identified patient

Requestor Consuming Gateway at NCP-B (service consumer at the country of care)

Input ListPatientRequest

Message

Body (1) Identifier of the patient whose patient summary is requested
 (2) Optional: epSOS CDA template qualifier (pivot and/or source coded document [1]). If no template qualifier is given the service provider MUST provide all available encodings.

Security Token [PT] X.509 NCP-B service certificate
 [ST] epSOS HCP Identity Assertion

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

[ST] epSOS Treatment Relationship
Confirmation Assertion [O]

Output Message in successful Case	ListPatientResponse
	Body
	(1) epSOS-encoded patient summary (CDA) or/and (2) source coded patient summary of the identified patient
	Security Token
	[PT] X.509 NCP-A service certificate
Precondition of success scenario	<p>In addition to the requirements stated in e1-REQ-4841 the following preconditions MUST be met for successful processing:</p> <p>Service consumer and service provider share a common identifier for the patient</p> <p>The patient has given consent to the use of epSOS</p> <p>A valid patient summary for the identified patient is accessible for NCP-A</p> <p>A treatment relationship exists between the patient and the requesting HP and the attesting assertion can be verified by the service provider</p> <p>The HP is authorised to access the requested data</p>
Main success scenario	<p>Actions of the epSOS Patient Service provider:</p> <p>Validate the authenticity of the service consumer</p> <p>Verify HCP identity assertion and TRC assertion</p> <p>Verify that the patient has given valid consent to epSOS and that the consent applies to the current usage scenario</p> <p>Retrieve patient's patient summary source document</p> <p>Enforce national security policy and (if available) patient privacy policy</p> <p>Verify authenticity and integrity of the patient summary</p> <p>Transform patient summary into epSOS pivot format (if requested and</p>

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

needed) and write a respective audit trail entry

Render PDF from source document (if requested and needed)

Apply epSOS protection means to the response message and send it to the requestor

Fault Conditions	<p>Preconditions for a success scenario are not met</p> <hr/> <p>Requestor has insufficient rights to access the patient's medical summary</p> <hr/> <p>No patient summary is available for the identified patient</p> <hr/> <p>No consent for patient summary sharing is registered for the identified patient</p> <hr/> <p>The patient summary cannot be provided in the requested encoding</p> <hr/> <p>Temporary failure (e. g. verification of preconditions cannot be performed due to a system failure)</p> <hr/>
------------------	--

[1] The term „source coded document“ is used for an encoding of a medical document that did not undergo any semantic translation. Following D3.5.2 it is assumed that PDF/A embedded within CDA is used as the format of choice for source coded documents.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.3 e1-FLD-78 Implementable Perspective

3.4.3.1 e1-FLD-162 Information Dimension

3.4.3.1.1 e1-REQ-2094 Patient Summary template conformance

Related to e1-REQ-3892 FR21: Patient Summary Conformance

Related to e1-REQ-4624 Information Model: Patient Summary & ePrescription

Related to e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-2074 CDA conformance

Related to e1-REQ-2076 Coded elements attributes optionality

Related to e1-REQ-2080 Consumer capabilities (epSOS PDF)

Related to e1-REQ-2079 Document Instance Identifier

Related to e1-REQ-2091 Element <translation>

Related to e1-REQ-2075 epSOS CDA Recipient Responsibilities

Related to e1-REQ-2097 epSOS pdf conformance

Related to e1-REQ-2082 epSOS PDF – epSOS pivot link

Related to e1-REQ-2081 Implementable Original document identification

Related to e1-REQ-2078 Link between coded elements and text

Related to e1-REQ-3894 Links among documents

Related to e1-REQ-2090 Recording of transcoded/translation data

Related to e1-REQ-2092 Reference coded system used in Country A

Related to e1-REQ-2095 Required Sections

Related to e1-REQ-2077 Valorization of displayName

epSOS Patient Summary SHALL be conformant with the template

1.3.6.1.4.1.12559.11.10.1.3.1.1.3 specification according to D3.9.1 Appendix B1.

The pdf documents should have the same header and simply the original documents scanned with the specification being based on the IHE:

Integrating the Healthcare Enterprise, Patient Care Coordination Technical Framework, Volume 1 and Volume 2- Revision 5, IHE International, August 10, 2009.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Integrating the Healthcare Enterprise, Patient Care Coordination CDA Content Modules- Trial Implementation Supplement, August 10, 2009.

3.4.3.1.1.1 e1-REQ-2095 Required Sections

Related to e1-REQ-2094 Patient Summary template conformance

The following sections - at least - shall be present in a Patient Summary document:

The Medication Summary Section 1.3.6.1.4.1.12559.11.10.1.3.1.2.3

The Allergies and Other Adverse Reactions Section 1.3.6.1.4.1.19376.1.5.3.1.3.13

The Coded List of Surgeries Section 1.3.6.1.4.1.19376.1.5.3.1.3.12

The Active Problems Section 1.3.6.1.4.1.19376.1.5.3.1.3.6

The Medical Devices Coded Section 1.3.6.1.4.1.12559.11.10.1.3.1.2.4

3.4.3.1.2 e1-REQ-4879 Patient Summary CDA Document and Code

epSOS Consumer Document	Display Name	Coding Scheme	Node Representation
Patient Summary	Patient Summary	2.16.840.1.113883.6.1	60591-5

3.4.3.1.3 e1-REQ-4891 Request Message

The list() request MUST be initiated by an HP in the country of care for retrieving the patient summary of an identified patient. The respective request message builds upon the IHE XCF Cross-Gateway Fetch request message.

The <AdhocQueryRequest> element that encapsulates the query parameters MUST be used as follows for epSOS:

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Element Name	epSOS Usage Convention
ResponseOption/@returnComposedObjects	MUST be "true"
ResponseOption/@returnType	MUST be "LeafClassWithRepositoryItem" (XCF)
AdhocQuery	Container for holding the ebML stored query arguments. All arguments MUST be encoded as query slots (see table below).
AdhocQuery@id	MUST be "urn:uuid:f2072993-9478-41df-a603-8f016706efe8" which indicates a Fetch (which is an adaption of the findDocuments Query as defined in ITI TF-2a:3.18.1, August 2009)

Only synchronous web services exchange MUST be used. The *XDS Affinity Domain Option* only applies to the national environment. Therefore it MUST NOT be used for NCP-2-NCP message exchange.

Stored query argument slots MUST be defined for the patient identifier and the document class code. The document format code and the document type code MAY be given. Other argument slots than the ones listed below MUST be ignored by the service provider and SHOULD NOT be issued by the service consumer.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Slot Name	Opt	Slot Value
\$XDSDocumentEntryPatientId	R	Equals to the patient identifier that was provided by the epSOS <i>Identification Service</i> (encoded as HL7 v3 II data type)
\$XDSDocumentEntryStatus	R	Only approved documents MUST be returned: 'urn:oasis:names:tc:ebxml-regrep: StatusType:Approved'
\$XDSDocumentEntryClassCode	R	Patient summary LOINC code ("60591-5") coded according to specification in ITI TF-2a: 3.18.4.1.2.3.4 Coding of Code/Code-Scheme. As classification scheme 2.16.840.1.113883.6.1 MUST be used: '60591-5^^2.16.840.1.113883.6.1'
\$XDSDocumentEntryTypeCode	O	Patient summary LOINC code ("60591-5") coded according to specification in ITI TF-2a: 3.18.4.1.2.3.4 Coding of Code/Code-Scheme. As classification scheme 2.16.840.1.113883.6.1 MUST be used: '60591-5^^2.16.840.1.113883.6.1'
\$XDSDocumentEntryFormatCode	O	Format qualifier as defined in table 1C of epSOS D3.5.2C; see table below for details on applying these codes to the retrieval of a patient's medical summary. Only encodings of the patient summary that comply to the requested format code will be returned by the service provider. If this stored query slot is omitted the service provider MUST deliver all available encodings.[1]

For the document format only the format codes defined in epSOS D3.5.2C and listed in the following table MUST be used.

Document Format	Format Code	Document content
epSOS pivot coded Patient Summary	urn:epsos:ps:ps:2010	HL7 CDA document acc. epSOS D3.5.2C. The patient's country of

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

		affiliation MUST be able to provide the patient's summarised medical data in this format.
PDF/A source coded document	urn:ihe:iti:xds-sd:pdf:2008	CDA-envelope PDF/A encoding of the original document without any semantic transformation of a patient summary as source coded PDF with a CDA header per IHE XDS-SD. The patient's country of affiliation SHOULD be able to provide the patient's summarised medical data in this format.

[1] Acc. to epSOS D3.2.2 countries MAY provide patient summary data only in epSOS pivot coded format. A query where the format code is omitted will in these case provide the same result as a query for the epSOS pivot coded document format only.

3.4.3.1.4 e1-REQ-4896 Response Message (Full Success Scenario)

Related to e1-REQ-4895 Expected Actions

Depending on the requested format code the epSOS list() response contains the epSOS pivot encoded patient summary document, the PDF/A encoded patient summary document or both documents of the identified patient. The respective message builds upon the IHE XCF Cross-Gateway Fetch response and Cross-Gateway Fetch Response messages [1].

The fields defined for the epSOS ListResponse message MUST be used as follows:

Element Name	epSOS Usage Convention
query:AdhocQueryResponse	Response message acc to IHE XCF Cross-Gateway Fetch response message IHE XCF
@status	For the full success scenario the response status MUST be set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" or "urn:ihe:iti:2007:ResponseStatusType:PartialSuccess"

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

	(for details see table below)
..../rs:RegistryErrorList	In case that a warning is given by the service provider, this element holds the respective warning codes and messages. It must be used acc. to section 4.1.13 of IHE ITI TF 3, October 2008.
..../rim:RegistryObjectList	This element MUST be provided for the full success scenario. It MUST at least contain one child <rim:ExtrinsicObject/> element.
.../..../rim:ExtrinsicObject	For each encoding of the patient summary a <rim:ExtrinsicObject/> element MUST be provided. Each <rim:ExtrinsicObject/> element is described and classified by metadata acc. to the table below.
.../.../..../rimext:Document	This element MUST appear as the last element child of an <rim:ExtrinsicObject/> element. It may appear zero or one times. This element contains the base 64 encoded content of the document. The document contents are associated with the DocumentEntry (ExtrinsicObject) metadata by the fact that it is nested inside it within the XML. The base64 encoded document content MAY be encrypted. How encryption is applied and how the encryption key is negotiated should be subject to an additional specification on advanced security safeguards.

Each provided patient summary encoding (epSOS pivot and/or source coded PDF) MUST be further classified by metadata. The following table lists the usage conventions that MUST be followed for the epSOS Patient Service response message. If not stated otherwise the classification schemes as defined in section 4.3.1.2 of IHE ITI TF 3 October 2008 MUST be used. If no restrictions on metadata values are given, the metadata elements MUST be used as per IHE XCF.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Metadata (ebRIM names)	Binding	epSOS Opt.	epSOS usage convention
status	Attribute	R	MUST be "urn:oasis:names:tc:ebxml-regrep>StatusType:Approved"
MimeType	Attribute	R	MUST be "text/xml" for both epSOS pivot CDA and CDA-wrapped PDF
Name	Main	R	MUST be "Patient Summary".
Description	Main	O	MAY be empty. MAY be ignored by the service consumer.
VersionInfo	Main	R	MUST be "1.1"
creationTime	rim:Slot	O	MAY be omitted by the service provider and MAY be ignored by the service consumer. If given, the value MUST be encoded as HL7 v2 Date Time "YYYY[MM[DD[hh[mm[ss]]]]]"
hash	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.
languageCode	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.
repositoryUniqueld	rim:Slot	O	COULD be omitted by the service provider and MAY be processed by the service consumer in an IHE-compatible NI-scenario.
serviceStartTime serviceEndTime	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

			consumer.
size	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.
sourcePatientId	rim:Slot	R	MUST contain the same value as XDSDocumentEntry.PatientId (see below).
sourcePatientInfo	rim:Slot	X	MUST NOT be used. Future versions of epSOS MAY define different protection levels for metadata and documents. Therefore all metadata elements that might carry medical or social information MUST be omitted.
classCode	Classification	R	Patient summary LOINC code ("60591-5"). As classification scheme "urn:oid:2.16.840.1.113883.6.1" MUST be used
eventCodeList	Classification	X	MUST NOT be used. Future versions of epSOS MAY define different protection levels for metadata and documents. Therefore all metadata elements that might carry medical or social information MUST be omitted.
author	Classification	X	MUST NOT be used. Future versions of epSOS MAY define different protection levels for metadata and documents. Therefore all metadata elements that might carry medical or social information MUST be omitted.
confidentialityCode	Classification	R	MUST be provided for XCF compatibility but MAY be ignored

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

			by the service consumer. Value SHOULD be set to "N", as long as the Minimal Metadata Profile is not published.
formatCode	Classification	R	MUST be "urn:epSOS:ps:ps:2010" for epSOS pivot CDA and "urn:ihe:iti:xds-sd:pdf:2008" for epSOS source coded PDF (see table 1C of epSOS D3.5.2C).
healthcareFacilityTypeCode	Classification	R	MUST be provided for XCF compatibility and correct addressing. Value MUST be set to ISO 3166-1 alpha-2 country code of the addressed PN.
practiceSettingCode	Classification	R	MUST be provided for XCF compatibility. Value MUST be set to "Not Used" in order to protect private patient information.
XDSDocumentEntry.uniqueId	ExternalIdentifier	R	MUST hold the OID of the document. The document unique id value MUST be the same as the value of the document's <ClinicalDocument/id> CDA header element.
XDSDocumentEntry.PatientId	ExternalIdentifier	R	MUST hold the patient identifier. The service consumer MUST verify that this id matches the patient Id that was discovered by the epSOS Identification Service.

Other metadata than the ones listed above SHOULD NOT be provided by the service provider and MUST NOT be processed by the service consumer.

By definition only a single patient summary is provided per patient. If two documents are provided in response to a Patient Service list request, these MUST be different encodings of the same patient's medical summary data (epSOS pivot coded and PDF/A source coded).

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

If document relationships are defined, an ebRIM association MUST be used for declaring the epSOS pivot coded document as a transformation of the source coded document. As classification scheme urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3 MUST be used per IHE XCF. "epSOS pivot" is defined as the only valid code value for the transformation:

```

<rim:Association id="id of the association"
  associationType="urn:ihe:iti:2007:AssociationType:XFRM"
  sourceObject="UUID of the source coded document"
  targetObject="UUID of the epSOS pivot document"
  objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
  <rim:Classification
    id="id of the classification"
    classificationScheme="urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3"
    classifiedObject="id of the association"
    objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
    nodeRepresentation="epSOS pivot">
    <rim:Slot name="codingScheme">
      <rim:ValueList>
        <rim:Value>epSOS translation types</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Name>
      <rim:LocalizedString value="Translation into epSOS pivot format"/>
    </rim:Name>
  </rim:Classification>
</rim:Association>

```

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Metadata (ebRIM names)	Binding	epSOS Opt.	epSOS usage convention
associationType	Attribute	R	MUST be "urn:ihe:iti:2007:AssociationType:XFRM"
sourceObject	Attribute	R	MUST be UUID of the source coded document
targetObject	Attribute	R	MUST be UUID of the epSOS pivot document
Association Documentation	Main	O	MAY be empty. MAY be ignored by the service consumer. MAY contain a description of the Association according to the Association Documentation object as used by IHE.
classificationSheme	classification	O	MUST be "urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3"
classifiedObject	Attribute	O	MUST be I.D. of the association
nodeRepresentation	Attribute	O	MUST be "epSOS pivot"
codingScheme	rim:Slot	O	MUST be "epSOS translation types" and "Translation into epSOS pivot format"

[1] The IHE XCF profile has been accepted and is currently in Trial Implementation.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.3.1.5 e1-REQ-4897 epSOS Patient Service Errors and Warnings

Related to e1-REQ-4895 Expected Actions

If a warning is to be transmitted to the HP the ebXML Registry Error mechanism MUST be used with a syntax as defined in section 3.43.5 of IHE ITI TF 2b August 2009. As the location of the warning is implied, the respective location attribute SHOULD be empty.

The following table lists the epSOS defined warning codes:

Warning Condition and Severity	Status	Message	Code
Not all of the requested encodings are provided (e.g. due to inability to transcode a certain national code). (ERROR)	PartialSuccess	Rendering incomplete	4101
The HP MUST consider additionally the source coded document because it MAY contain information that is not included in the epSOS pivot CDA (e.g. because field were nullified due to missing code mappings) (WARNING)	Success	Source coded document must be considered	2102

If the *epSOS Patient Service* provider is unable to respond with the patient's summarised medical data in the requested encoding it MUST respond with a ListResponse message that only contains a <AdhocQueryResponse/RegistryResponse> element. For a full list of error messages defined for IHE X* see table 4.1-11 in IHE ITI TF-3 October 2008. The following table lists the additional, epSOS-specific response status types and error/warning/info codes to be used within the <RegistryErrorList> element.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

Condition and Severity	Response Status	Message	Code	Action to be taken
The patient has not given consent to the requested service. (ERROR)	Failure	No Consent	4701	The HP SHOULD ask the patient to give consent to the requested service in country B. If the patient gives consent, the consent MUST be transmitted to country-A by using the respective operation of the epSOS consent service. If such consent giving procedure is accepted by country A, HP SHOULD re-issue the request for medical data.
Country A requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	Failure	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechanism (e.g. smartcard) and re-issue the request with the respective identity assertion.
Either the security policy of country A or a privacy policy of the patient (that was given in country A) does not allow the requested operation to be performed by the HP (ERROR).	Failure	Insufficient Rights	4703	If the HP can switch to another (appropriate) role, he SHOULD do so and re-issue the request.
No patient summary is registered for the given patient. (WARNING)	Success	No Data	1102	-

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3		
		Version: 1.0		
D5.2.3		Date: 31/01/2013		

If PDF-coded patient summary is requested: Country A does not provide the (optional) source coded version of the patient summary (INFO)	Success	Unsupported Feature	4201	The service consumer SHOULD re-issue the request with another encoding.
The query argument slots used by the service consumer are not supported by the service provider. (ERROR)	Failure	Unknown Signifier	4202	The service consumer SHOULD re-issue the request with another set of query arguments.
The requested encoding cannot be provided due to a transcoding error. (ERROR)	Failure	Transcoding Error	4203	The service consumer SHOULD re-issue the request with another encoding.
The service provider is unable to evaluate the given argument values (ERROR).	Failure	Unknown Filter	4204	The service consumer MAY re-issue the request using another filter expression.

3.4.3.1.6 e1-REQ-4887 epSOS Patient Service Security Audit Considerations

Related to e1-REQ-1838 epSOS HCP Assurance Audit Schema

Related to e1-REQ-1839 epSOS Patient Privacy Audit Schema

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in e1-REQ-1838. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in e1-REQ-1839.

The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

 epsOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

epsOS Instance	Opt.	Description
Event	R	Audited event
Requesting Point of Care	R / X	HPO that issued the original request. This category MUST be filled by the service consumer. It MUST NOT be provided by the service provider.
Human Requestor	R	HP that triggered the request
Source Gateway	R	Service consumer node address at the country of Care
Target Gateway	R	Service provider node address at the country of the patient's affiliation
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	R	Patient
Event Target	R	Subject to the Query
Error Message	O	Only used in case that the request handling was not completed successfully

For the Event Target Category the following fields MUST be provided:

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "24" (Query)
ParticipantObjectIDTypeCode	R	MUST be "10" (Search Criteria)
ParticipantObjectID	R	MUST be string-encoded UUIDs of the returned documents

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.4.3.1.7 e1-TXT-755 Example Request Message

The following excerpt from an *epSOS Patient Service* list() request message shows a cross-NCP query request that contains argument slots for retrieving the patient summary (LOINC code 60591-5) of an identified patient (patient identifier 90378912821). In this example the service consumer does not specify the requested encoding. Therefore the service provider delivers all available encodings (e. g. epSOS pivot and source coded document) according to e1-REQ-4891.

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" ... >
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
  <query:AdhocQueryRequest>
    <query:ResponseOption returnComposedObjects="true"
                           returnType="LeafClassWithRepositoryItem"/>
    <rim:AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-
a90016b0af0d">
      <rim:Slot name="$XDSDocumentEntryPatientId">
        <rim:ValueList>

<rim:Value>'90378912821^^^&#1.3.6.1.4.1.21367.2005.3.7&#ISO'
          </rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="$XDSDocumentEntryStatus">
        <rim:ValueList>
          <rim:Value>('urn:oasis:names:tc:ebxml-
regrep>StatusType:Approved')
          </rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="$XDSDocumentEntryClassCode">
        <rim:ValueList>
          <rim:Value>('60591-5^^2.16.840.1.113883.6.1')</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <!-- Include associations whose sourceObject and targetObject
attributes
          reference ExtrinsicObjects returned -->
    </rim:AdhocQuery>
    </query:AdhocQueryRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.4.3.1.8 e1-TXT-756 Example Response Messages

The following message is a possible response to the sample request message given in e1-TXT-755. The patient's country of affiliation responds with both encodings. No MTOM optimization has been done (since this is a wire-format only optimization).

```

<soapenv:Envelope>
  <soapenv:Header>....</soapenv:Header>
  <soapenv:Body>
    <query:AdhocQueryResponse
      status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">

      <rim:RegistryObjectList>

        <!-- epsos pivot CDA patient summary document -->
        <rimext:ExtrinsicObject
          id="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
          lid="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
          objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
          status="urn:oasis:names:tc:ebxml-
regrep:StatusType:Approved"
          mimeType="text/xml">

        <!-- These attributes are required by XCA but not used by
epsos.
          They will be ignored by the epsos service consumer
(NCP-B) -->

        <rim:Slot name="creationTime">
          <rim:ValueList>
            <rim:Value>20100524</rim:Value>
          </rim:ValueList>
        </rim:Slot>

        <rim:Slot name="languageCode">
          <rim:ValueList>
            <rim:Value>en-us</rim:Value>
          </rim:ValueList>
        </rim:Slot>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<!-- set to same value as Patient ID (required by XCA) -->
<rim:Slot name="sourcePatientId">
    <rim:ValueList>

<rim:Value>90378912821^^^&#1.3.6.1.4.1.21367.2005.3.7&#ISO</rim:
Value>
    </rim:ValueList>
</rim:Slot>

<rim:Name>
    <rim:LocalizedString xml:lang="en" charset="UTF-8"
        value="Patient Summary"/>
</rim:Name>

<rim:Description/>
<rim:VersionInfo versionName="1.1"/>

<!-- HealthcareFacilityType Code -->
<rim:Classification
    id="urn:uuid:5c678da8-6ffa-4a85-90f6-cb2f914d482f"
    lid="urn:uuid:5c678da8-6ffa-4a85-90f6-cb2f914d482f"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:f33fb8ac-18af-42cc-
ae0e-ed0b0bdb91e1"
    classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481"
    nodeRepresentation="Not Used">
    <rim:Slot name="codingScheme">
        <rim:ValueList>
            <rim:Value>
                epSOS Healthcare Facility Type Codes-Not
Used
                </rim:Value>
            </rim:ValueList>
        </rim:Slot>
        <rim:Name>
            <rim:LocalizedString xml:lang="en" charset="UTF-8"
                value="Not Used"/>
        </rim:Name>
    </rim:Classification>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<!-- PracticeSetting Code -->
<rim:Classification
    id="urn:uuid:b01599e3-79a6-4322-b5fc-f32ada9ee7f4"
    lid="urn:uuid:b01599e3-79a6-4322-b5fc-f32ada9ee7f4"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
        classificationScheme="urn:uuid:cccf5598-8b07-4b77-
a05e-ae952c785ead"
        classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481"
        nodeRepresentation="Not Used">
<rim:Slot name="codingScheme">
    <rim:ValueList>
        <rim:Value>
            epSOS Practice Setting Codes-Not Used
        </rim:Value>
    </rim:ValueList>
</rim:Slot>
<rim:Name>
    <rim:LocalizedString xml:lang="en" charset="UTF-8"
        value="Not Used"/>
</rim:Name>
</rim:Classification>

<!-- Confidentiality Code -->
<rim:Classification
    id="urn:uuid:d0dc74b9-f013-4639-b9c2-fac2420af0dd"
    lid="urn:uuid:d0dc74b9-f013-4639-b9c2-fac2420af0dd"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
        classificationScheme="urn:uuid:f4f85eac-e6cb-4883-
b524-f2705394840f"
        classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481"
        nodeRepresentation="Not Used">
<rim:Slot name="codingScheme">
    <rim:ValueList>
        <rim:Value>
            epSOS Confidentiality Codes-Not Used
        </rim:Value>
    </rim:ValueList>
</rim:Slot>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<rim:Name>
    <rim:LocalizedString xml:lang="en" charset="UTF-8"
        value="Not Used"/>
</rim:Name>
</rim:Classification>

<!-- End of attributes not used by epSOS -->

<!-- Class Code - (60591-560591-5) -->
<rim:Classification
    id="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
    lid="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:41a5887f-8865-4c09-
adf7-e362475b143a"
    classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481"
    nodeRepresentation="60591-5">
    <rim:Slot name="codingScheme">
        <rim:ValueList>
            <rim:Value>2.16.840.1.113883.6.1</rim:Value>
        </rim:ValueList>
    </rim:Slot>
    <rim:Name>
        <rim:LocalizedString xml:lang="en" charset="UTF-8"
            value="Patient Summary"/>
    </rim:Name>
</rim:Classification>

<!-- Type Code - (60591-5) -->
<rim:Classification
    id="urn:uuid:87a7cfcc2-a956-4d6e-af30-c7e78809c95f"
    lid="urn:uuid:87a7cfcc2-a956-4d6e-af30-c7e78809c95f"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:f0306f51-975f-434e-
a61c-c59651d33983"
    classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481"
    nodeRepresentation="60591-5">
    <rim:Slot name="codingScheme">

```

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

```

<rim:ValueList>
    <rim:Value>2.16.840.1.113883.6.1</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
    <rim:LocalizedString xml:lang="en" charset="UTF-8"
        value="Patient Summary"/>
</rim:Name>
</rim:Classification>

<!-- Format Code -->
<rim:Classification
    id="urn:uuid:ae68bdf8-4f32-4829-8313-2dd39ea3ab2d"
    lid="urn:uuid:ae68bdf8-4f32-4829-8313-2dd39ea3ab2d"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:a09d5840-386c-46f2-
b5ad-9c3699a4309d"
    classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481"
    nodeRepresentation="epSOS coded summary">
    <rim:Slot name="codingScheme">
        <rim:ValueList>
            <rim:Value>epSOS formatCodes</rim:Value>
        </rim:ValueList>
    </rim:Slot>
    <rim:Name>
        <rim:LocalizedString xml:lang="en" charset="UTF-8"
            value="epSOS Coded Summary"/>
    </rim:Name>
</rim:Classification>

<!-- Patient ID -->
<rim:ExternalIdentifier
    id="urn:uuid:982f1551-5901-4bc5-8870-801181941817"
    lid="urn:uuid:982f1551-5901-4bc5-8870-801181941817"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
    identificationScheme="urn:uuid:58a6f841-87b3-4a3e-
92fd-a8ffff98427"
    value="90378912821^^^&#13.6.1.4.1.21367.2005.3.7&#13;ISO"

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

        registryObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481">
            <rim:Name>
                <rim:LocalizedString xml:lang="en-us"
charset="UTF-8"
                    value="XDSDocumentEntry.patientId"/>
            </rim:Name>
        </rim:ExternalIdentifier>

        <!-- Unique ID -->
        <rim:ExternalIdentifier
            id="urn:uuid:c67e3a92-5300-448d-9af2-0a37e9f129bf"
            lid="urn:uuid:c67e3a92-5300-448d-9af2-0a37e9f129bf"
            objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
            identificationScheme="urn:uuid:2e82c1f6-a085-4c72-
9da3-8640a32e42ab"
            value="1.42.20100103225206.3.3"
            registryObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481">
            <rim:Name>
                <rim:LocalizedString xml:lang="en-us"
charset="UTF-8"
                    value="XDSDocumentEntry.uniqueId"/>
            </rim:Name>
        </rim:ExternalIdentifier>

        <!-- Document contents, before MTOM optimization -->
        <rimext:Document>
            UjBsR09EbGhz0dTQUxNQUFBUNBRU1tQ1p0dU1GUUhEUzhi.....
        </rimext:Document>
    </rimext:ExtrinsicObject>

    <!-- epsOS source coded PDF patient summary document -->
    <rimext:ExtrinsicObject
        id="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-d355b57a5016"
        lid="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-d355b57a5016"
        objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
        status="urn:oasis:names:tc:ebxml-
regrep:StatusType:Approved"
        mimeType="text/xml">

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

<!-- These attributes are required by XCA but not used by epSOS.

They will be ignored by the epSOS service consumer
(NCP-B) -->

```

<rim:Slot name="creationTime">
    <rim:ValueList>
        <rim:Value>20100524</rim:Value>
    </rim:ValueList>
</rim:Slot>

<rim:Slot name="languageCode">
    <rim:ValueList>
        <rim:Value>en-us</rim:Value>
    </rim:ValueList>
</rim:Slot>

<!-- set to same value as Patient ID (required by XCA) -->
<rim:Slot name="sourcePatientId">
    <rim:ValueList>
        <rim:Value>
90378912821^^^&#x1D;1.3.6.1.4.1.21367.2005.3.7&#x1D;ISO
        </rim:Value>
    </rim:ValueList>
</rim:Slot>

<rim:Name/>
<rim:Description/>
<rim:VersionInfo versionName="1.1"/>

<!-- HealthcareFacilityType Code -->
<rim:Classification
    id="urn:uuid:7dda3d1e-8d96-4fee-b691-f1810d44bc8d"
    lid="urn:uuid:7dda3d1e-8d96-4fee-b691-f1810d44bc8d"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:f33fb8ac-18af-42cc-
ae0e-ed0b0bdb91e1"
    classifiedObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016"
    nodeRepresentation="Not Used">

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<rim:Slot name="codingScheme">
    <rim:ValueList>
        <rim:Value>
            epsOS Healthcare Facility Type Codes-Not
Used
        </rim:Value>
    </rim:ValueList>
</rim:Slot>
<rim:Name>
    <rim:LocalizedString xml:lang="en" charset="UTF-8"
        value="Not Used"/>
</rim:Name>
</rim:Classification>

<!-- PracticeSetting Code -->
<rim:Classification
    id="urn:uuid:89a73ab3-344a-4098-b827-ac8dea078ef"
    lid="urn:uuid:89a73ab3-344a-4098-b827-ac8dea078ef"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:cccf5598-8b07-4b77-
a05e-ae952c785ead"
    classifiedObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016"
    nodeRepresentation="Not Used">
    <rim:Slot name="codingScheme">
        <rim:ValueList>
            <rim:Value>
                epsOS Practice Setting Codes-Not Used
            </rim:Value>
        </rim:ValueList>
    </rim:Slot>
    <rim:Name>
        <rim:LocalizedString xml:lang="en" charset="UTF-8"
            value="Not Used"/>
    </rim:Name>
</rim:Classification>

<!-- Confidentiality Code -->
<rim:Classification
    id="urn:uuid:fa176711-e83a-4fb2-95a3-a4810b0351fa"
    lid="urn:uuid:fa176711-e83a-4fb2-95a3-a4810b0351fa"
```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:f4f85eac-e6cb-4883-
b524-f2705394840f"
        classifiedObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016"
            nodeRepresentation="Not Used">
                <rim:Slot name="codingScheme">
                    <rim:ValueList>
                        <rim:Value>
                            epSOS Confidentiality Codes-Not Used
                        </rim:Value>
                    </rim:ValueList>
                </rim:Slot>
                <rim:Name>
                    <rim:LocalizedString xml:lang="en" charset="UTF-8">
                        value="Not Used"/>
                </rim:Name>
            </rim:Classification>

<!-- End of attributes not used by epSOS --&gt;

<!-- Class Code - Patient Summary (60591-5) --&gt;
&lt;rim:Classification
    id="urn:uuid:8a07ab13-1685-452f-9363-c89a37d9eb5b"
    lid="urn:uuid:8a07ab13-1685-452f-9363-c89a37d9eb5b"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:41a5887f-8865-4c09-
adf7-e362475b143a"
        classifiedObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016"
            nodeRepresentation="60591-5"&gt;
                &lt;rim:Slot name="codingScheme"&gt;
                    &lt;rim:ValueList&gt;
                        &lt;rim:Value&gt;2.16.840.1.113883.6.1&lt;/rim:Value&gt;
                    &lt;/rim:ValueList&gt;
                &lt;/rim:Slot&gt;
                &lt;rim:Name&gt;
                    &lt;rim:LocalizedString xml:lang="en" charset="UTF-8"&gt;
                        value="Patient Summary"/&gt;
                &lt;/rim:Name&gt;
</pre>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

        </rim:Classification>

        <!-- Type Code - Patient Summary (60591-5) -->
        <rim:Classification
            id="urn:uuid:c7cffb04-3537-4e8b-963d-f2f639c734de"
            lid="urn:uuid:c7cffb04-3537-4e8b-963d-f2f639c734de"
            objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
            classificationScheme="urn:uuid:f0306f51-975f-434e-
a61c-c59651d33983"
            classifiedObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016"
            nodeRepresentation="60591-5">
            <rim:Slot name="codingScheme">
                <rim:ValueList>
                    <rim:Value>2.16.840.1.113883.6.1</rim:Value>
                </rim:ValueList>
            </rim:Slot>
            <rim:Name>
                <rim:LocalizedString xml:lang="en" charset="UTF-8">
                    value="Patient Summary"/>
            </rim:Name>
        </rim:Classification>

        <!-- Format Code -->
        <rim:Classification
            id="urn:uuid:ca064887-589c-408a-be6f-b7844f473ee6"
            lid="urn:uuid:ca064887-589c-408a-be6f-b7844f473ee6"
            objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
            classificationScheme="urn:uuid:a09d5840-386c-46f2-
b5ad-9c3699a4309d"
            classifiedObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016"
            nodeRepresentation="urn:ihe:iti:xds-sd:pdf:2008">
            <rim:Slot name="codingScheme">
                <rim:ValueList>
                    <rim:Value>epSOS formatCodes</rim:Value>
                </rim:ValueList>
            </rim:Slot>
            <rim:Name>
                <rim:LocalizedString xml:lang="en" charset="UTF-8">

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

        value="PDF/A Coded Document"/>
    </rim:Name>
</rim:Classification>

<!-- Patient ID -->
<rim:ExternalIdentifier
    id="urn:uuid:27d19a5d-7850-4c37-9499-a42fe6fdd5c8"
    lid="urn:uuid:27d19a5d-7850-4c37-9499-a42fe6fdd5c8"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
    identificationScheme="urn:uuid:58a6f841-87b3-4a3e-
92fd-a8ffeff98427"

value="90378912821^^^&#1.3.6.1.4.1.21367.2005.3.7&#ISO"
    registryObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016">
    <rim:Name>
        <rim:LocalizedString xml:lang="en-us"
charset="UTF-8"
            value="XDSDocumentEntry.patientId"/>
    </rim:Name>
</rim:ExternalIdentifier>

<!-- Unique ID -->
<rim:ExternalIdentifier
    id="urn:uuid:81854cc8-2b26-45d6-8132-9f9c7eb2e5ae"
    lid="urn:uuid:81854cc8-2b26-45d6-8132-9f9c7eb2e5ae"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
    identificationScheme="urn:uuid:2e82c1f6-a085-4c72-
9da3-8640a32e42ab"
    value="1.42.20100103225206.3.2"
    registryObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016">
    <rim:Name>
        <rim:LocalizedString xml:lang="en-us"
charset="UTF-8"
            value="XDSDocumentEntry.uniqueId"/>
    </rim:Name>
</rim:ExternalIdentifier>

<!-- Document contents, before MTOM optimization -->
```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

```

<rimext:Document>
    UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUUhEUzhi....
</rimext:Document>
</rimext:ExtrinsicObject>

<rim:Association id="urn:uuid:f4618a30-a7fb-49a3-b27f-
d1994b9c4e32"
    lid="urn:uuid:f4618a30-a7fb-49a3-b27f-d1994b9c4e32"
    status="urn:oasis:names:tc:ebxml-
regrep:StatusType:Approved"
    associationType="urn:ihe:iti:2007:AssociationType:XFRM"
    sourceObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-
01d7b6b0f481"
    targetObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016">
    <rim:Classification
        id="urn:uuid:8ec64c7e-8b7d-4d63-8741-c5a5890e5af3"
        lid="urn:uuid:8ec64c7e-8b7d-4d63-8741-c5a5890e5af3"
        classificationScheme="urn:uuid:abd807a3-4432-4053-
87b4-fd82c643d1f3"
        classifiedObject="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-
d355b57a5016"
        objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
        nodeRepresentation="epSOS pivot">
        <rim:Slot name="codingScheme">
            <rim:ValueList>
                <rim:Value>epSOS translation types</rim:Value>
            </rim:ValueList>
        </rim:Slot>
        <rim:Name>
            <rim:LocalizedString
                value="Translation into epSOS pivot format"/>
        </rim:Name>
    </rim:Classification>
</rim:Association>

</rim:RegistryObjectList>
</query:AdhocQueryResponse>
</soapenv:Body>
</soapenv:Envelope>

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.4.3.2 e1-FLD-171 Computational Dimension

3.4.3.2.1 e1-REQ-4886 epSOS Patient Service Message Specification

Related to e1-REQ-4840 epSOS PatientService Service Interface & Functional Specification

Related to e1-REQ-4883 epSOS Trusted Service List

The *epSOS Patient Service* MUST be used to share an identified patient's medical summary between the patient's country of affiliation and the country of care. Both countries are represented by their respective NCPs.

The implementation of the epSOS Patient Service is based on the following standards:

ebRIM: OASIS/ebXML Registry Information Model v3.0 OASIS ebRIM 3.0

ebRS: OASIS/ebXML Registry Services Specifications v3.0[1] OASIS ebRS 3.0

MTOM: SOAP Message Transmission Optimization Mechanism W3C MTOM

XOP: XML-binary Optimized Packaging W3C XOP

and is based on the following IHE profile:

XCF: IHE Cross-Community Fetch IHE XCF

For discovery and localisation of the Patient Service instance that is responsible for providing access to the identified patient's data see e1-REQ-4883.

[1] The integration of ebRS and MTOM as used by epSOS is not compatible with the current version of OASIS ebRS. Support for MTOM will be part of the forthcoming ebRS v4.0.

3.4.3.2.1.1 e1-REQ-4890 List() Operation

The *epSOS Patient Service* list() operation is implemented as IHE XCF Cross-Gateway Fetch transaction. It is fully compliant with the ebRS 3.0 standard. The *epSOS Patient Service* list() operation includes the documents listed in the response meta-data, just like they would have been included in Cross-Gateway Fetch (SOAP 1.2 MTOB with XOP encoding attachments).

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

3.4.3.2.1.1.1 e1-REQ-4895 Expected Actions

Related to e1-REQ-3876 NFR01- Service availability

Related to e1-REQ-3885 NFR10- Guaranteed delivery

Related to e1-REQ-4897 epSOS Patient Service Errors and Warnings

Related to e1-REQ-4860 Exception Handling

Related to e1-REQ-4896 Response Message (Full Success Scenario)

The *epSOS Patient Service* provider shall respond to a ListRequest message with the ListResponse message containing

the identified patient's patient summary document(s) together with a status notification (full success scenario) or

an error message (no patient summary provided).

The *epSOS Patient Service* provider MUST verify that the requesting service user has sufficient rights to access the full patient summary of the identified patient.

In case of an error that relates to the transmission of the request or the processing of the epSOS security token, the *epSOS Patient Service* provider MUST respond with a fault message according to e1-REQ-4860.

3.4.3.2.2 e1-REQ-4888 epSOS Patient Service Protocol Requirements

Related to e1-REQ-1883 epSOS Common Message Format

The *epSOS Patient Service* List() request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in e1-REQ-1883.

Port types and bindings MUST be used as defined in the WSDL given in e1-REQ-4889. Acc. to this the *epSOS Patient Service* List() operation's request and response data MUST be contained within the message body as follows:

epSOS Patient Service	Message Body
List request	CrossGatewayQueryRetrieve_Message (see e1-REQ-4889)
List response	CrossGatewayQueryRetrieveResponse_Message (see e1-REQ-4889)

The request message MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in e1-REQ-4884. The response message

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in e1-REQ-4884.

3.4.3.2.2.1 e1-REQ-4889 IHE XCA Responding Gateway Query-Retrieve WSDL

```

<?xml version="1.0" encoding="UTF-8"?>
<definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:ihe="urn:ihe:iti:xds-b:2007" xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
  xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
  xmlns:xdsext="urn:ihe:iti:xds-ebrim:extensions:2010"
  targetNamespace="urn:ihe:iti:xds-b:2007"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
  name="RespondingGateway_QueryRetrieve">
  <documentation>IHE XCA Responding Gateway Query Retrieve</documentation>
  <types>
    <xsd:schema elementFormDefault="qualified">
      <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
        schemaLocation="../schemas/rs.xsd"/>
      <xsd:import namespace="urn:ihe:iti:xds-b:2007"
        schemaLocation="../schemas/XDS.b_DocumentRepository.xsd"/>
      <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
        schemaLocation="../schemas/query.xsd"/>
    </xsd:schema>
  </types>
  <message name="CrossGatewayQueryRetrieve_Message">
    <documentation>Cross Gateway Query Retrieve</documentation>
    <part name="body" element="query:AdhocQueryRequest"/>
  </message>
  <message name="CrossGatewayQueryRetrieveResponse_Message">
    <documentation>Cross Gateway Query RetrieveResponse</documentation>
    <part name="body" element="query:AdhocQueryResponse"/>
  </message>
  <portType name="RespondingGatewayQueryRetrieve_PortType">
    <operation name="RespondingGateway_CrossGatewayQueryRetrieve">
      <input message="ihe:CrossGatewayQueryRetrieve_Message"
        wsaw:Action="urn:ihe:iti:2010:CrossGatewayQueryRetrieve"/>
      <output message="ihe:CrossGatewayQueryRetrieveResponse_Message"
        wsaw:Action="urn:ihe:iti:2010:CrossGatewayQueryRetrieveResponse"/>
    </operation>
  </portType>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<binding name="RespondingGatewayQueryRetrieve_Binding_Soap12"
    type="ihe:RespondingGatewayQueryRetrieve_PortType">
    <soap12:binding style="document"
        transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="RespondingGateway_CrossGatewayQueryRetrieve">
        <soap12:operation
            soapAction="urn:ihe:iti:2010:CrossGatewayQueryRetrieve"/>
        <input>
            <soap12:body use="literal"/>
        </input>
        <output>
            <soap12:body use="literal"/>
        </output>
    </operation>
</binding>
<service name="RespondingGatewayQueryRetrieve_Service">
    <port name="RespondingGatewayQueryRetrieve_Port_Soap12"
        binding="ihe:RespondingGatewayQueryRetrieve_Binding_Soap12">
        <soap12:address
            location="http://servicelocation/RespondingGatewayQueryRetrieve_Service"/>
    </port>
</service>
</definitions>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.5 e1-FLD-65 eP/eD

3.5.1 e1-FLD-79 Conceptual Perspective

3.5.1.1 e1-FLD-127 Information model

3.5.1.1.1 e1-REQ-1670 About the prescription data in the ePrescription

Related to e1-REQ-4546 FR09- Prescription presentation

Related to e1-REQ-4550 FR13- Identification of the medicinal product

Related to e1-REQ-4626 Information Model: Patient Summary & ePrescription

Variable	Definitions	Optional	Comments	Example
Prescription ID	Identification of the prescription	Req		
Prescription Item ID	Identification of the Item within the prescription	Req	One prescription might contain more than one item (or medicines). In the country where prescriptions contain just one item or medicine, then the prescription ID=Prescription ID item	Item1: medicinal product 1 description+posology Item2: Medicinal product 2 description+posology Item 1 ID:1234 Item 2 ID: 2345
Country A Cross-border/regional/national medicinal product	Code that identifies the medicinal product description in that	Opt	Some countries like Denmark and	

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

code Country B Single concept	<p>region/country or among some countries</p> <p>It is the translation to a single concept in country B from the epSOS semantic format. This is not a mapping to the existing medicinal products in country B</p>	Sweden might have the same medicinal product code	
		This is not a field but a block of information made up of the following fields. If a single prescription is made in country A, in country B can not be several prescriptions. It has to be one for practical reasons and then a brand name among all available in country B should be selected. Please refer to Table 2 for clarification on this concept	Paracetamolo0,5g 30 tablets (the original medicinal product prescribed in country A is Termalgin 500 mg 30 comprimidos)
		Req	Country B translates
- Active ingredient (of country A in Country	Is defined as a substance that alone or		Paracetamolo

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

B units)	in combination with one or more other ingredients produces the intended activity of a medicinal product.		(does not change) the active ingredient from country A to country B units (single concept) but it is the same active ingredient. This is part of FR 13 (Id of medicinal product)	
- Strength of the medicinal product (of country A in Country B units)	Is the content of the active ingredient expressed quantitatively per dosage unit, per unit of volume or per unit of weight, according to the pharmaceutical dose form.	Req	Country B translates (does not change) the strength from country A to country B units (single concept) but it is the same strength This is part of FR 13 (Id of medicinal product)	Dose/unit. E.g. 500mg that it is what contains 1 tablet,i.e. the unit in country A, it can be 0,5g in country B
- Medicinal product package (of country A)	Delivery unit of a medicinal product in an outer container.	Req	This is the size of the package prescribed in Country A.	30

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

- Pharmaceutical dose form (of country A in Country B units)	<p>A Pharmaceutical Dose Form is the form in which a pharmaceutical product is presented in the medicinal product package as supplied by the marketing authorization holder/manufacturer/distributor.</p>		This is part of FR 13 (Id of medicinal product) and FR14 (substitution)	
		Req	<p>Country B translates the dose form from country A to country B units (single concept) but it is the same pharmaceutical dose form.</p> <p>This is part of FR 13 (Id of medicinal product)</p>	In country A is 'comprimidos' and in country B 'tablets'
		Opt	<p>This is a free text field and can be empty if the prescription was made by active ingredient</p>	Termalgin
Brand name of the medicinal product prescribed in country A	<p>The name, which may be either an invented name not liable to confusion with the common name, or a common or scientific name accompanied by a trade mark or the name of the marketing authorisation holder.</p>	Opt		
		Opt		
Route of Administration	Indicates the part of the body through or into	Country B translates the	In injectable: intramuscular	

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

(of country A in Country B units)	which, or the way in which, the medicinal product is intended to be introduced. In some cases a medicinal product can be intended for more than one route and/or method of administration.		route of administration from country A to country B units but it is the same route	In Tablet: oral
Number of packages (of country A)	Number of boxes that have been prescribed in country A	Req	This is the number of boxes prescribed in country A	2
Posology (of country A in Country B units)	Number of units per intake, frequency of intakes (per day/month or week) and duration of treatment.	Req	Country B translates the posology from country A to country B units but it is the same posology. This field can be a single field or a block of different fields (Number of units per intake, frequency of intakes (per day/month or week) and duration of treatment)	1 unit/intake every 24 hrs for a duration of 30 days in country A can be 1unit/intake once a day during 1 month

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

Date of issue of the prescription Date of onset of treatment Date of end of treatment Instructions to patient Advise to the dispenser	<p>Date when the prescription was made</p> <p>Date when patient needs to start taking the medicine prescribed</p> <p>Date when patient has to finish taking the medicine prescribed</p> <p>The prescriber might give to the patient instructions</p> <p>The prescriber might give instructions to the dispenser</p>	Req		
		Opt		Date
		Opt		Date
		Opt	They must be presented in the original language.	Take only when headache
		Opt	The information will be in the original language as automatic translation is not secure enough. To avoid legal and ethical issues to the dispenser, it should be wise to implement an option that allows the dispenser to decide,	Watch hypertension

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

		knowing that this data is available, whether he wants to consult it or not.	
--	--	---	--

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version: 1.0
D5.2.3	Date: 31/01/2013

3.5.1.1.2 e1-REQ-3984 About the dispensed medicine data

Related to e1-REQ-4552 FR15- Dispensed medicine information sent to country A

Related to e1-REQ-4626 Information Model: Patient Summary & ePrescription

Variable	Definitions	MS/Max	Comments	Example
		MS Minimum Data Set Max Maximum		
Dispensed medicine Id	Identification of the dispensed medicine event in country B	MS		
Prescription ID	Identification of the related prescription (country A) of the dispensed medicine	MS	This is part of FR 16 (Id of prescription and medicine dispensed)	
Prescription Item ID	Identification of the item or medicine of the related prescription (country A) of the dispensed medicine	MS	One prescription might contain more than one item or medicine. In the country where prescriptions contain just one item, then the prescription ID=Prescription ID item. This is part of FR 16 (Id of prescription and medicine dispensed)	
Country B Cross-border/regional/national medicinal	Code that identifies the medicinal product description in that region/country or among some countries	Max	Some countries like Denmark and Sweden might have the same medicinal product code	

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

product code				
Country A Single concept	It is the translation to a single code in country A from the epSOS semantic format	MS	If a single medicine is dispensed in country B, in country A can not be several dispensed medicines. It has to clearly identify the active ingredient of the medicine dispensed.	Paracetamol 500 mg 20 comprimidos
Active ingredient	Is defined as a substance that alone or in combination with one or more other ingredients produces the intended activity of a medicinal product.		This is the active ingredient of the medicine dispensed in Country B (in Country A units), that has to be the same that the one prescribed as substitution is not allowed.	Paracetamol
Strength of the medicinal product	Is the content of the active ingredient expressed quantitatively per dosage unit, per unit of volume or per unit of weight, according to the pharmaceutical dose form.		Strength of the medicinal product of the medicine dispensed in Country B (in Country A units) that has to be the same that the one prescribed.	500 mg
Medicinal product package (of country B)	Delivery unit of a medicinal product in an outer container.		As substitution of package size is in the scope, the size of the package of the medicine dispensed may differ from the one prescribed	20
Pharmaceutical dose	A Pharmaceutical Dose Form is the form in which		This is the pharmaceutical dose	Comprimidos

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3	
	Version:	1.0
D5.2.3	Date:	31/01/2013

form	a pharmaceutical product is presented in the medicinal product package as supplied by the marketing authorization holder/manufacturer/distributor.		form of the medicine dispensed in Country B (in Country A units), that has to be the same than the one prescribed.	
Route of Administration	Indicates the part of the body through or into which, or the way in which, the medicinal product is intended to be introduced. In some cases a medicinal product can be intended for more than one route and/or method of administration.	Max	As substitution of route of administration is out of the scope, the route of administration of the medicine dispensed has to be the same than the one prescribed	In injectable: intramuscular In Tablet: oral
Number of packages	Number of boxes that have been dispensed	MS	This is part of FR 16 (Id of prescription and medicine dispensed). In principle, the number of packages dispensed should be the same than the ones prescribed for patient safety reasons but this might be subject to legal restrictions that will need to be followed during the pilot.	2
Date of the dispensed medicine event	Date when the medicine was dispensed	MS		
Substitution	If a different brand name or	Max	It indicates if brand	YES/NO

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

	package size has been dispensed		name or package size dispensed are different from the one prescribed. This is part of FR 14 (substitution)	
--	---------------------------------	--	---	--

Apart from the previous data elements, also a copy of the original medicine dispensed has to be available in country A (this is the same data elements, structured or not, but without any semantic transformation, so it includes the brand name of the medicine dispensed).

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.5.1.1.3 e1-REQ-5141 About Patient Identification in the ePrescription

Synchronized with e1-REQ-1668 About Patient Identification in the ePrescription

Variable	Definitions	MS: Minimum Optional	Comments	Example
Given Name	The Name of the patient	Yes	This field can contain more than one element	Marta
Family Name/Surname	The surname/s of the patient	Yes	This field can contain more than one element	Español Smith
Gender	The gender of the patient	Yes		Male/female/unknown
Birth date	Date of birth	Yes	This field may contain only the year	01/01/2009
Regional/National Health Id	If the patient has a regional or national Health Identification	Yes	This field is required by some national laws	
Social/Insurance Number		Yes	If a patient has both, national/regional ID and Social/Insurance number, only the regional/national Health Id is required by law. If the only identification the patient has is the Social/insurance number, then this one is considered as the regional/national Health Id. This field is required by some national laws.	

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version: 1.0
D5.2.3	Date: 31/01/2013

3.5.1.1.4 e1-REQ-5143 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-1669 About HP Prescriber Identification in the ePrescription

Variable	Definitions	MS: Minimum Max: maximum	Comments	Example
Given Name	The Name of the Prescriber	MS	This field can contain more than one element	Marta
Family name/surname	The surname/s of the Prescriber	MS	This field can contain more than one element	Español Smith
HP Id number	The identification of the person as HP	MS		12345
Profession		MS		Physician
Specialist		Max		Dermatologist
Prescriber Facility Address:	The place (complete address) where the prescriber made the prescription		<p>This is not a field but a block of information made up of the following fields.</p> <p>This might not be in the dataset but this information needs to be available for the process traceability</p>	e.g., Los Bermejales Health Care Centre. Alemania St. Seville, 41018. Spain

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

			(FR20)	
Name of the Facility		Max		For instance, the name of the building: Los Berrmejales
Street Address		Max		Alemania Street
City		Max		Seville
State or Province		Max		Seville
Zip or Postal Code		Max		41018
Telephone		Max		+34 954123123
Contact email of the centre or of the prescriber		Max		losbermejaleshealthcentre@xxx.es
Country	The country where the prescription was made	MS	The dispenser needs to know the country where he is consulting the information from	Spain
Prescriber Organization:			This is not a field but a block of information made up of the following fields. This might not be in the dataset but this information needs to be available for the	

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

			process traceability (FR20)	
Organization Name		Max		e.g. Andalusia Health Service
Organization Identifier		Max	This field can be numbers and/or letters	123458xfs

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

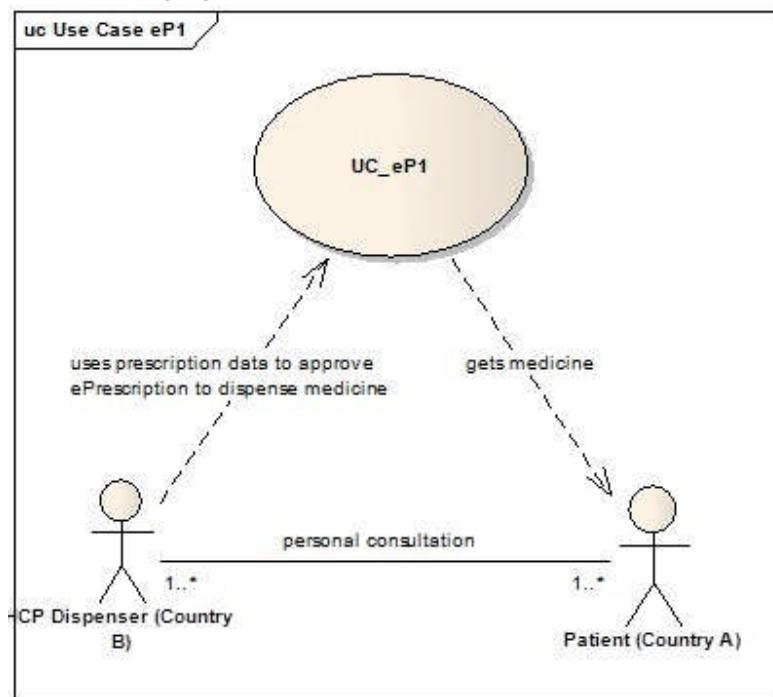
3.5.1.2 e1-FLD-128 Computational Dimension

3.5.1.2.1 e1-REQ-4457 ePrescription Use Case "Medicine already prescribed in country A"

Based on e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

A patient needs medicine that has already been prescribed in country A when in country B. In this case the HP Dispenser should be able to electronically access the prescription from the same eHealth interface she uses for prescriptions ordered in the local country. When medicine is dis-patched, the system should notify the patient's NCP in country A about the dispensed drugs.

The following figures show the use case and the sequence diagram:



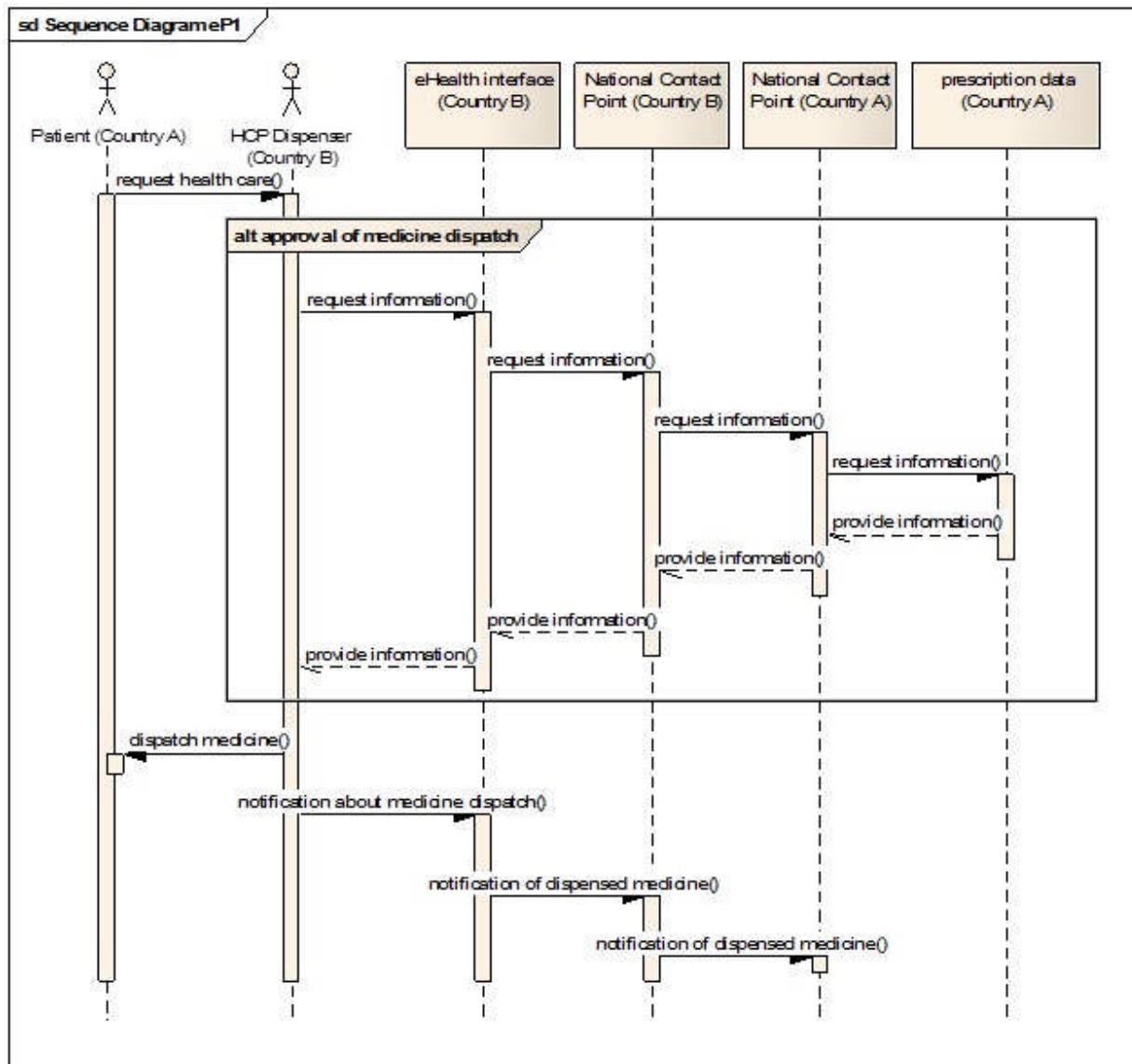
Use Case ePrescription “A patient needs medicine that is already prescribed in country A when in country B”

According to the use case description the HP Dispenser (e.g. pharmacist) must know what medicine has been prescribed (e.g. through a consultation).

The HP Dispenser accesses the necessary data to be able to dispatch the medicine. After the medicine is dispensed the system informs the NCP in country A about the dispatch.

The following figure shows the interaction between the different entities of the use case.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



Sequence Diagram ePrescription “A patient needs medicine that is already prescribed in country A when in country B ”

Based on the sequence diagram the steps within this use case are shown in the following table.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Step	Name	Description	Output	Entities
1	Patient requests health care	A patient from country A requests health care in form of consultation from a HCP in country B.	Trigger to HCP Dispenser	Patient, HCP Dispenser
2	HCP Dispenser requests information	The HCP Dispenser requests information about a prescription via an eHealth-interface.	Information request to prescription record	HCP Dispenser, eHealth-interface
3	NCP transfer 1	The eHealth interface transfers the request via the NCP B to NCP A which transfers it to the prescription data for response	Information transfer to prescription data	eHealth interface, NCP A, NCP B, prescription data
4	NCP transfer 2	NCP A receives an response from prescription data and transfers it to NCP B	Information transfer from prescription data	NCP A, NCP B, prescription data
5	Response from prescription data	The NCP B transfers the response to the eHealth interface.	Response to the eHealth interface	NCP B, eHealth interface
6	Dispatch of medicine	With the necessary information from the prescription data the medicine can be dispatched.	Dispatch medicine	HCP Dispenser, patient
7	Notification of dispatched medicine	The NCP A is notified about the dispatched medicine through NCP B.	Message to NCP A	eHealth-interface, NCP A, NCP B

Sequence diagram ePrescription “A patient needs medicine that is already prescribed in country A when in country B”

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.1.2.2 e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Related to e1-REQ-4542 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-4558 Data Integrity

Related to e1-REQ-4563 Data Origin and Data Authenticity

Related to e1-REQ-2085 eP is not a collection of patient prescriptions

Based on e1-REQ-4457 ePrescription Use Case "Medicine already prescribed in country A"

Related to e1-REQ-4545 FR08- Information selection

Related to e1-REQ-4546 FR09- Prescription presentation

Related to e1-REQ-4547 FR10- 'Available' (and thus, valid) prescription

Related to e1-REQ-4548 FR11- Access to current prescriptions by dispenser

Related to e1-REQ-4549 FR12- Original prescription

Related to e1-REQ-4550 FR13- Identification of the medicinal product

Related to e1-REQ-4551 FR14- Substitution

Related to e1-REQ-4552 FR15- Dispensed medicine information sent to country A

Related to e1-REQ-4553 FR16- Univocal relation between original prescription and medicinal product dispensed

Related to e1-REQ-4554 FR17- Original dispensed medicine

Related to e1-REQ-4555 FR20- Information Traceability

Related to e1-REQ-4538 HP-B Identification and Authentication

Related to e1-REQ-4539 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-4557 NFR01- Service availability

Related to e1-REQ-4559 NFR03- Response time

Related to e1-REQ-4561 NFR05- Access control

Related to e1-REQ-4565 NFR09- Trust between countries

Related to e1-REQ-4566 NFR10- Guaranteed delivery

Related to e1-REQ-4567 NFR11- Single session

Related to e1-REQ-4568 NFR12- Supervision services

Related to e1-REQ-4540 Patient Identification

Related to e1-REQ-4596 REQ 3.3.11 Notification with eDispensation document

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Related to e1-REQ-4544 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-4543 Structured Information and Semantic Compliance

Related to e1-REQ-4671 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-4560 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-4541 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-4629 epSOS DispensationService Service Interface & Functional Specification

Related to e1-REQ-4628 epSOS OrderService Service Interface & Functional Specification

This use case describes the dispensing of medicine(s) in country B when the medicine(s) has been prescribed in a different country (country A), where the patient has a valid identification in terms of healthcare. Country A in this case is also the country where the patient can be univocally identified.

In order for the Use case to take place, several preconditions are needed:

The patient has already been electronically prescribed (valid prescription) by a prescriber authorised to prescribe in country A.

In country B, a mechanism to validate the identity of the patient and to handle patient consent against country A has to be available at the pharmacy and the dispenser is a person legally authorised to dispense medicinal products.

In order to obtain the needed information in country B, the Prescription Provider in country A must make accessible at least the 'available' prescriptions to be sent or requested by another country. This implies that country A is able to calculate the 'available' prescriptions (it has the necessary information or parameters to select the prescriptions that can be dispensed at that moment).

Country A must provide, maintain and support a logical country node (NCP) supporting communication of the information identified in this section with country B and vice versa and that there must be a chain of trust between system actors in this process.

If these preconditions are met, the use case can take place.

The first thing the patient needs to do is to identify himself to the dispenser.

The dispenser has to check if this identification is valid or not through his Dispense provider before accessing to any data. In order to avoid legal issues, it is imperative that the patient is univocally identified so that patient identity can be ensured. The appropriate method to achieve this will be specified later on in the corresponding work package (WP3.6 'Identity Management').

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Once the patient has been identified, the HP can ask for the ‘available’ prescriptions for that patient. It must be clear to the HP and the patient what information is going to be asked for and what information is going to be presented to the HP.

Before any information is presented to the HP, patient consent must be given (the appropriate method will be specified in WP3.6 ‘Identity Management’).

Access to ‘available’ prescriptions:

In order to select the prescription requested by the patient, the list of ‘available’ (and thus, time valid) prescriptions from country A has to be presented to the dispenser and the patient. These prescriptions are provided by country A according to the rules that apply in its health system, meaning that only a prescription that can be dispensed in country A at that moment is available for dispensing in country B (this implies that country A is responsible for deciding which prescriptions are available to be dispensed in country B and thus, all prescriptions that pharmacists see in country B can be dispensed to the patient at that moment). The prescription has to be valid and is within the correct time slot defined for collection from the Pharmacy for country A (in some countries, mainly with long term treatments, the prescriptions can only be collected from pharmacies within specific date/time slots to help the patient correctly administer the medicine(s)).

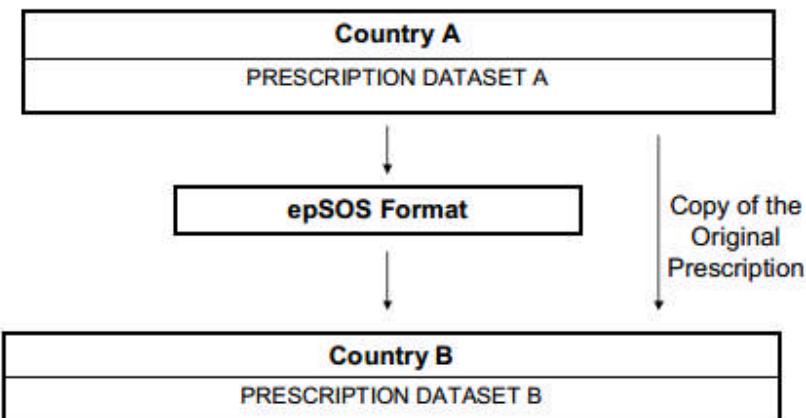
If there are no ‘available’ prescriptions, the HP will be informed of that.

Once the information requested has been sent from country A to country B, to allow the dispenser to understand the information, this must be intelligible to him, i.e. structured, equivalent meaning and understandable, presented in his system as decided by country B (in order to ease the process for the HP, it is recommended that the information is presented as it is normally done) and contain all necessary information to identify the right medicine.

As the medicinal products are not the same in the different countries, to guarantee the univocal identification of a medicinal product cross border, the nomenclature to be used for the name must be the active ingredient and not the brand name. The following scenario is assumed on the process of sending the prescription dataset from country A to country B:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Data set interoperability



The information that country A is sending to country B will need to identify the active ingredient of the medicinal product. Then, it will be converted to a common epSOS format (to be defined by WP3.5 'Semantic Services') to be sent to country B. Country B will then receive the prescription data set of country A in this common epSOS format. This epSOS format will afterwards need to be translated in the NCP to a single concept in country B (if a single prescription is made in country A, in country B can not be several prescriptions for practical reasons) and then a brand name among all available in country B should be selected. The reason is that normally, the same medicinal product does not exist (this document covers substitution of brand name and/or size of package) in both countries and country B will need to translate its single code into a medicinal product that exists in there (brand name (different from the original) + strength + pharmaceutical dose form + package size (than can be different from the original)).

The following table represents the state chart of the prescription when sent to country B:

Country A medicinal product	Country A single concept (identifies active ingredient)	epSOS format	Country B single concept	Country B medicinal product
Termalgin 500 mg 30 comprimidos	Paracetamol 500 mg 30 comprimidos	xxx	Paracetamolo 0,5g 30 tablets	Paracetamolo Tesco 0,5g 20 tablets

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

Some issues might arise when translating the medicine from country A to country B. The different possibilities are described:

- In country B the exact same branded medicine does exist, meaning that the exact same following elements are found: active ingredient + brand name + strength + pharmaceutical dose form + package size. The dispenser then dispenses the medicine.
- In country B the same medicine in generic form does exist, meaning that the exact same following elements are found: active ingredient + strength + pharmaceutical dose form + package size. The dispenser then dispenses the medicine and indicates to the Dispense provider that substitution (of brand name) has taken place. When brand name substitution is of a product with a narrow therapeutic index and/or release, characteristics may be altered by a switch and patient safety considerations must be taken into account as alteration may result in either toxicity or under treatment.
- In country B the medicine does exist but with different package size. The dispenser might then dispense another size of package (either smaller or bigger) according to country B rules or legislation and will indicate to the Dispense provider that substitution (of package size) has taken place⁵. The consequence of changing the package size affects to the use case at different levels:
 - o the patient gets less medicine than needed (if the package dispensed is smaller than the original size)
 - o if the size of the package dispensed in country B does not exist in country A, this will affect to the update of the prescription (to calculate the new credit or medicine left to be taken).
 - o The countries need to be able to recognise or translate the original medicine independently of the Package size so it can be changed (if WP3.5 ‘Semantic Services’ decides to codify several fields –group them- in a single code (e.g. active ingredient + strength + ...=1234), the package size can not be part of this single code to allow substitution.
- In country B the medicine does not exist, meaning the active ingredient or strength or pharmaceutical dose form is not the same. In this case, the dispensing is not possible as substitution of any of these three elements is out of the scope of the epSOS LSP. The dispenser has to see and be aware that there is an available prescription but that can not be translated into a medicinal product in country B as the active ingredient or the strength or the pharmaceutical dose form is not the same. Some countries ‘group’ different pharmaceutical dose forms into one, which can be considered for other countries as a ‘change’ of the dose form. In Andalusia for instance, when a ‘gastric-resistant tablet’ is prescribed, this is converted to ‘tablet’ (as ‘gastric-resistant tablet’ belongs to the ‘tablet’ group). This grouping is within the scope of epSOS LSP.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

In order to help preventing these issues, country B has to receive also the original prescription written in country A. This “copy” of the unchanged original prescription from country A may be used by the pharmacist in country B when accessing to the ‘available’ prescriptions as a manual safety/security check of, for instance, the original brand name or the pharmaceutical dose form. Also, to avoid these issues, a group of experts (clinicians and pharmacists) could be created that control:

- which therapeutic groups can be substituted and which not (e.g. antiepileptic, cardiotonic...)
- the level of detail of description of the data elements regarding semantics (e.g. active ingredient or active ingredient + salts). It might happen that for some therapeutic groups only active ingredient is needed and for others is important to have also the salts).
- the possible grouping of pharmaceutical dose forms. As some countries group them and the criteria to group is different as the clinical criteria is also different, it should be advisable to have a common and homogenised understanding of the grouping, e.g. group the pharmaceutical dose forms based on the route of administration so countries can still group following the national criteria.

Special attention will need to be paid during the piloting phase to prevent any possible breach in the security of the patient.

Once the patient and the dispenser agree on the prescription (in order to do that, both have to understand the information), this one is about to be dispensed according to country B legislation which implies some legal issues that might be faced during the process (a deeper analysis is made in Annex III):

- The first issue that will need to be solved is the countries’ and European’s legislation regarding the legal validity of ePrescriptions (both the local and the foreign versions). If a country A ePrescription is not recognised in country B, there is no use case.
- That the prescription does not contain all necessary fields needed by law in country B. Although this issue has been considered when selecting the minimum dataset of the prescription to be sent to country B, there might be countries that are not able to provide all these fields, resulting on the pharmacist being unable to dispense. The result of this situation will need to be followed and analysed during the piloting phase.
- That substitution is performed in country B when in country A substitution of that specific medicine is not allowed. Country A must be aware of this possibility when signing up the contractual agreements for the pilot operation (e.g., when country B group the pharmaceutical dose form).

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

- Another important issue is the validity as an order (time valid, prescribed by an authorised person, under country A legal framework, can be dispensed at that moment to the patient – intervals between regular dispenses...) and the veracity of data of a country A prescription in country B (country A will need to assure this two aspects of the prescriptions before sending them to country B, i.e. calculate the 'available' prescriptions). This means that pharmacists in country B could question:
 - o that the prescription is not time valid for country B. This can have a major impact on long term treatments and chronic patients as for every country the duration of these treatments is different.
 - o that it was made for instance by a nurse, where in country B nurses are not allowed to prescribe. In this case the impact is, so far, low as not in many countries nurses are, right now, allowed to prescribe, but the patient will then need to go to the prescriber to get a new prescription;
 - o to dispense more than x boxes of the medicine, even if it is indicated in the prescription, as by law they are not permitted to dispense more than x. This will result in the patient having to go back to the pharmacy another day(s) to collect further boxes having a major impact on patients with long term conditions that are going to be present in country B for some time;
 - o if the medicine can be dispensed as this medicine, when prescribed in country B, needs a special 'ok' or additional authorization before being dispensed. This will have a major impact on the patient as he will need to go to the prescriber to be prescribed as he needs the medicine;
 - o to dispense the medicine as brand name or package size substitution is not permitted at the point of dispensing. This has a huge impact on country B as pharmacists will not be able to dispense any medicine at all (the likelihood of requiring brand name substitution is really high);
 - o to dispense the medicine as brand name is compulsory and the country A prescription has been made by active ingredient. This situation has a major impact for those patients coming from regions or countries that prescribe by active ingredient (e.g. Andalusia).
- The legal principle is that country A sets the validity when prescribing and country B when dispensing. All these specific situations will need to be analysed during the piloting phase to be able to evaluate the real impact of legislation on the ePrescription service level.
- The HP dispenses the medicine to the patient and must enter the information into the system to inform country A.. The process in country B then ends unless the patient wants to withdraw more medicines or has further requests to the pharmacist that needs to keep the access to the patient's information, i.e., the HP does not have access anymore to patient information unless

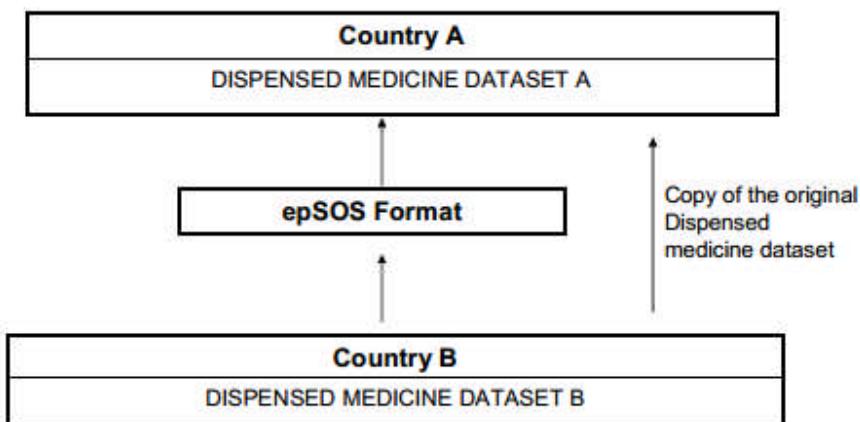
 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

identification and patient consent is performed again. Before the patient leaves the pharmacy, the pharmacist should inform, if possible, that the information of the event has been sent to country A. Patient data can be saved in the HP system if the patient gives consent (consent has to be explicit, freely given and informed) and if country B can assure the proper measures to deal with clinical information according to the Data Protection Legislation. In order to guarantee the security of the patient, country B must assure that country A has successfully received the information about the medicine(s) dispensed before requesting again the ‘available’ prescriptions of that patient to country A. Country A must assure that the ‘available’ prescriptions have been updated with that information before informing country B of the successful receipt.

The information about the medicine dispensed that has been sent to country A must support the identification of the related prescription in country A to allow updating the original prescription and for things like brand name, package size substitution etc.

The following scenario is assumed on the process of sending the dispensed medicine information from country A to country B:

Data set interoperability



The dispensed medicine information will be converted to a common epSOS format (to be defined by WP3.5 ‘Semantic Services’) to be sent to country A. Country A will then receive a dispensed medicine data set of country B in an epSOS format. As in most cases, the same medicinal product does not exist (this document covers different brand name and/or size of package) in both countries, country A will translate the epSOS format into the single concept of the related prescription. In consequence, and for security and traceability reasons, also a copy of the original medicinal product dispensed in country B (the dispensed medicine data set B)

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

has to be sent to country A so the real information of what has been dispensed is available in country A. Country A then can decide whether to include this information on its Systems or not but always assuring the proper measures to keep or to deal with clinical information according to its Data Protection Legislation.

The following table represents the state chart of the dispensed medicine when sent to country A

Country B medicinal product dispensed	Country B single concept (identifies active ingredient of the medicine dispensed)	epSOS format	Country A single concept
Paracetamolo Tesco 0,5g 20 tablets	Paracetamolo 0,5g 20 tablets	xxx	Paracetamol 500 mg 20 comprimidos

During the process, the dispenser may identify that he does not have sufficient or all the necessary information required to support dispensing or considers for some reason not to dispense due to safety reasons. This has to be communicated to the patient. This situation will need to be analysed during the piloting phase to understand the reasons to not dispense.

3.5.2 e1-FLD-80 Logical Perspective

3.5.2.1 e1-TXT-533 Note

It has to be differentiated between requirements or functionalities and between data elements in the data set. They are complementary. I.e. not all FRs are translated into an element in the dataset. Also, the data set is focused on the prescription as such, not on the process, that again, are complementary. Also, the dataset identified in D3.1.2 is not a CDA document, it is Information that country A and B have to provide, and in some cases, not necessarily as a specific field in a CDA doc, i.e. it is important also to differentiate the clinical needs (D3.1.2) from the implementation of these needs (HL7, CDA, portal B...).

For all these points it is recommend to read section 5.2.1.2 of D3.1.2 as it makes an analysis of the process, describing all different possibilities and helps understand the requirements.

3.5.2.2 e1-REQ-4538 HP-B Identification and Authentication

Synchronized with e1-REQ-1981 HP-B Identification and Authentication

Tested by e1-REQ-5176 HP-B Identification and Authentication

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The identity and authenticity of an HP MUST be verified before he can use epSOS cross-border services. Each data access request MUST contain sufficient and verifiable information about (the identity and the role of) the accessory for assessing a country-A national security policy.

3.5.2.2.1 e1-TXT-627 Note

Associated Goals:

To provide security to the process.

To ensure that the HP is legally allowed to perform the functionalities described in this document.

Prevention of disclosure to unauthorized persons.

Actors: HP-B, NCP-B

3.5.2.3 e1-REQ-4539 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-2206 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Tested by e1-REQ-5178 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

epSOS agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations must be secured and codes of conduct as part of the epSOS Information Governance must be elaborated.

3.5.2.3.1 e1-TXT-628 Note

Associated Goals:

To avoid having to identify all professionals and institutions from a foreign country in the country of origin. On the one hand, each HP will be unequivocally identified and authenticated in his local system and must be identified based on his/her role/profile. On the other hand, Health Care Provider Organisation provides HP a status, a function, an authentication from which the HP trust is derived. Furthermore, Health Authorities Institutions assign and assure the status, the role, and sometimes the authentication of HP.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Actors: HP-B with rights for accessing eP, NCP-A, NCP-B

3.5.2.4 e1-REQ-4540 Patient Identification

Synchronized with e1-REQ-1973 Patient Identification

Tested by e1-REQ-5177 Patient Identification

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The intended recipient of medical data MUST identify the patient with sufficient accuracy. Medical data MUST only be disclosed after the patient was identified with sufficient accuracy.

Technical means for patient identification MUST NOT use or disclose medical data about this patient. Patient identifiers SHOULD NOT technically enable any unlawful linkage of the patient's medical data to other sanctioned personal data beyond any legitimate purpose from other domains. If technical means for identity protection (e.g. pseudonymization) are used, these MUST NOT disqualify the responsible parties to lawfully provide the patient access to his/her data. The original identification of the patient MUST NOT rely on the existence of electronic identifiers (eIDs). epsOS use cases MAY define further constraints on the accuracy and means of patient identification for that specific use case (e.g. identification by name considered as insufficient for the 112 use case).

3.5.2.4.1 e1-TXT-629 Note

Associated Goals:

To have certainty of the identity of the patient

Actors: HP-B with rights for accessing eP, NCP-A, NCP-B

3.5.2.5 e1-REQ-4560 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-1977 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Tested by e1-REQ-5194 Willful Disclosure (Data Confidentiality)

Medical data MUST NOT be disclosed to persons or organization unless they have been authorized by the patient (see »Consent-2; PIN«) and the disclosure is legally or explicitly required for fulfilling the treatment.

Medical data MUST NOT be disclosed to others than healthcare professionals or healthcare

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

professional organizations in any case.

Medical data MUST NOT be transferred to other destinations unless this disclosure has been authorized by the patient or is mandated by national law.

The proper enforcement of the willful disclosure acc. to »consent-2« MUST be controllable and verifiable by the patient.

Implications:

Data MUST be encrypted during transfer and whenever it is stored at (intermediate) nodes outside the trusted environment of an HP (see "IT-Systems directly controlled by HPs").

Depending on how "controllable" and "verifiable" are defined this requirement as well implies a need for secure end-to-end encryption between trusted HP environments.

3.5.2.5.1 e1-TXT-656 Note

3.5.2.6 e1-REQ-4541 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Tested by e1-REQ-5179 Willful Provisioning of Data (»Consent-1«)

The provisioning of medical data for cross-border medical use cases MUST require a willful and documentable act of agreeing by the patient.

This willful act MUST fulfill all requirements of an informed, free consent acc. to country-A legislation. It MUST deliver an appropriate level of data security and privacy for the patient as it is defined in his home country.

This willful act MUST be designed in full anticipation of a cross-border health data exchange scenario.

The respective consent MUST be given in written form and MUST be signed by the patient. A qualified digital signature MAY be used instead of a wet signature.

A country MUST assure that patient data is only accessible if a valid patient consent for data provisioning exists. A country MUST ensure that data is no longer accessible after the respective consent has been revoked or expired.

A HP- B is not required to explicitly verify the existence of a patient's »consent-1« (that was formerly given in country-A) as it is assumed that all epSOS country-A have established secure processes for enforcing the revocation of consents and therefore will not provide data to a country-B unless a valid »consent-1« exists.

3.5.2.6.1 e1-TXT-630 Note

Associated Goals:

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Manifesting the legal foundation for a lawful data processing

Granting the patient his specific rights according to data protection regulations

Deciding on whether a certain request for data is legitimated by the consent or not

Actors: Patient, HP-B, NCP-A, NCP-B

3.5.2.7 e1-REQ-4542 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

Tested by e1-REQ-5180 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Triggering a cross-country transfer of medical data MUST require a willful act by the patient.

This willful act MUST express the patient's explicit authorization to allow an identifiable healthcare professional the execution of defined data access operations.

This willful act MUST express the explicit authorization of the patient to transfer medical data to the formerly identified and specifically documented destination.

Countries MAY require that this willful act is documented by an explicit, written and informed consent that is to be signed by the patient.

Implications:

The authorization to perform a specific operation can only be given and documented in country-B (as this authorization requires the identification of both the patient and the HP-B).

Therefore epSOS MUST provide technical means to transmit information about the authorization/PIN to country-A before or while a data access operation is triggered.

3.5.2.7.1 e1-TXT-631 Note

Associated Goals:

Manifesting the legal foundation for a lawful data processing.

Granting the patient his specific rights according to data protection regulations.

Deciding on whether a certain request for data is legitimated by the consent or not.

Actors: Patient, HP-B, NCP-A, NCP-B

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

This requirement is subject to legal aspects defined in WP2.1 'Analysis of legal and regulatory issues' and the different solutions to handle it are described in WP3.6 'Identity Management'.

3.5.2.8 e1-REQ-4543 Structured Information and Semantic Compliance

Synchronized with e1-REQ-1983 Structured Information and Semantic Compliance

Tested by e1-REQ-5181 Structured Information and Semantic Compliance

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

epSOS MUST define the structure and semantics of all document types which are required to be shared cross-border within epSOS use cases (pivot schema and common terminologies).

It is the responsibility of each PN to preserve the semantics of original data when this is transformed and transcoded into the common epSOS format as defined for the respective document type. Transformation services within a country and epSOS semantic services should guarantee the smoothest semantic transformation, keeping the meaning and the value of the source document, considering the liability for the transformation, and assuring the reproducibility of the semantic transformation.

3.5.2.8.1 e1-TXT-632 Note

Associated Goals:

Safety reason

HP and patient understand the meaning of all the fields that are going to be shown to them

To provide the HP with the necessary information to safely dispense to the patient

Guarantee the safety of the patient through a proper understanding of the received information

Ensure safety delivery of care to patients thanks to the faithful exchange of meanings between systems and between systems and people

Actors: NCP-A, NCP-B

There are several possibilities to deal with the unified meanings regarding medicines:

Each data field of the minimum dataset defined in section 6 is translated into a common terminology or nomenclature.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

A subgroup of the minimum dataset (e.g. active ingredient + strength + pharmaceutical dose form) have a unique coding into the common language (this subgroup is the data that the doctor can not break up as they are defined by the commercialised products).

3.5.2.9 e1-REQ-4544 Semantic Interoperability of Structured Clinical Content

Synchronized with e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Tested by e1-REQ-5182 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Medical information shared among countries MUST be understandable (in the correct context) for the receiver. HP-B MUST be enabled to view and/or process medical documents encoded in a way that best matches the document structure and clinical terms that are commonly used in country-B.

Implications:

epSOS MUST provide semantic services that allow for translation/mapping of clinical terms. epSOS SHOULD use a common pivot schema and terminology set in order to limit the number of mappings that have to be defined and maintained.

3.5.2.9.1 e1-TXT-633 Note

Associated Goals:

Safety reason

HP and patient understand the meaning of all the fields that are going to be shown to them

To provide the HP with the necessary information to safely dispense to the patient

Guarantee the safety of the patient through a proper understanding of the received information

Ensure safety delivery of care to patients thanks to the faithful exchange of meanings between systems and between systems and people

Actors: NCP-A, NCP-B

e.g. the field 'active ingredient' means the same in both countries.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.5.2.10 e1-REQ-5132 Minimum and Maximum Data Sets

Synchronized with e1-REQ-1986 Minimum and Maximum Data Sets

Tested by e1-REQ-5183 Minimum and Maximum Data Sets

Every PN MUST provide means that enable an HP IT-System to properly translate, display and process mandatory data entries within epSOS documents. Every PN SHOULD provide means that enable an HP IT-System to properly translate, display and process optional data entries within epSOS documents.

PN MAY define additional data entries within epSOS documents as long as this does not violate the defined pivot schema. PN that receive such extended documents MAY ignore all data elements not defined by epSOS.

3.5.2.11 e1-REQ-4545 FR08- Information selection

Tested by e1-REQ-5155 FR08 - Information selection

Related to e1-REQ-4547 FR10- 'Available' (and thus, valid) prescription

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The information regarding the 'available' prescriptions and the current prescriptions must be well identified so the Dispenser knows what sort of information he is going to access or is looking at.

3.5.2.11.1 e1-TXT-634 Note

Associated Goals:

For safety reasons

To ease the process for the dispenser

Actors: Dispenser, Dispense provider

Available prescriptions are the ones that according to country A administration routines and legislation, can be dispensed at that specific moment to the patient. In Spain for instance, it is normally 1 box as long term prescriptions are for 1 year and the patient collects the medicines in specific periods according to the administration routine. In other countries like Sweden, patient can collect at one time up to a specific number of boxes.

Current prescriptions are all medicines that the prescriber has prescribed and patient is supposed to be taking at that moment

In the case that the prescription contains several items, there will be a set of patient, prescriber and prescription data per item.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.12 e1-REQ-4546 FR09- Prescription presentation

Related to e1-REQ-1670 About the prescription data in the ePrescription

Related to e1-REQ-2093 eP template conformance

Tested by e1-REQ-5156 FR09 - Prescription presentation

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The minimum data set as identified within D3.1.2 chapter 6.1 MUST be available to the dispenser at the time of dispensation.

3.5.2.12.1 e1-TXT-635 Note

Associated Goals:

To help the dispenser to choose the right data or piece of information.

To reduce time in dispensing

Actors: Dispense provider, Dispenser, NCPs

If there is more than one prescription 'available', the data related to identification of patient, prescriber and prescription MUST be provided per prescription 'available'

In the case that the prescription contains several items, there will be a set of patient, prescriber and prescription data per item.

3.5.2.13 e1-REQ-4547 FR10- 'Available' (and thus, valid) prescription

Related to e1-REQ-4545 FR08- Information selection

Tested by e1-REQ-5157 FR10- 'Available' (and thus, valid) prescription

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The dispenser MUST be able to see at least the "available prescriptions" of the patient in country A, i.e. the prescriptions that can be dispensed at that specific or particular moment. This means that the patient SHOULD be able to obtain in country B what he could have obtained in country A.

Country A MUST be able to calculate the 'available' prescriptions. In the case of a prescription for long term treatment, this MUST NOT only be the prescriptions that are time valid, but also those that can be withdrawn at that moment by the patient.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.5.2.13.1 e1-TXT-636 Note

Associated Goals:

For the dispenser to identify which prescription can be dispensed for that patient at that moment under country A conditions (country B then will dispense according to his legislation –to be further described)

To avoid problems of country A and B different prescription validity periods

Actors: Dispenser, Dispense provider, NCPs

This has some implications, already described in D3.1.2 section 5.2.1.2, some of which can be solved in the epSOS LSP and some others not.

That the patient has 3 packages prescribed does not necessarily mean that he can collect all at any day or the same day. There are several possibilities, f.i.:

He can collect all packages whenever he wants until a limit date

He can collect the packages, up to a max. number, only at specific slots of time

3.5.2.14 e1-REQ-4548 FR11- Access to current prescriptions by dispenser

Tested by e1-REQ-5195 FR11 - Access to current prescriptions by dispenser

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The Dispenser MAY consult the current prescriptions for that patient.

3.5.2.14.1 e1-TXT-637 Note

Associated Goals:

check possible interactions, pharmaceutical care, 'emergency dispense' (depending on country B legislation)

safety reasons

Actors: Dispenser, Dispense provider, NCPs

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.15 e1-REQ-4549 FR12- Original prescription

Related to e1-REQ-1988 Peering Original Document

Related to e1-REQ-4628 epSOS OrderService Service Interface & Functional Specification

Tested by e1-REQ-5158 FR12 - Original prescription

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The HP must be able to consult a copy of the original prescription (no epSOS semantic transformation) including at least the medicinal product description and the posology.

3.5.2.15.1 e1-TXT-638 Note

Associated Goals:

For safety reasons as the brand name of the product is probably going to be changed

Actors: Dispenser, Dispense provider, NCPs

When the eP is sent to country B, there is going to be a semantic transformation, starting from the mapping from local terminology to epSOS and from epSOS to terminology in country B (not the case for portal B but YES if integrated in dispensing system of B). In these semantic transformation processes, some information might be lost or altered.

Also, some dispense systems present to the pharmacist a list of commercial matches related to the original eP so pharmacist can choose which commercial product to dispense. If a prescription from another country is received, it might happen that in country B the exact same product does not exist, so the dispense system could show the closest match (in epSOS pilot, just brand name and package size) so the original medicinal product prescribed has been altered.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.16 e1-REQ-4550 FR13- Identification of the medicinal product

Related to e1-REQ-1670 About the prescription data in the ePrescription

Related to e1-REQ-2093 eP template conformance

Tested by e1-REQ-5159 FR13 - Identification of the medicinal product

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The dispenser MUST have in the prescription the minimum dataset as defined in D3.1.2 chapter 6.1 in order to identify the correct product (active ingredient, strength, pharmaceutical dose form...) to be safely dispensed.

3.5.2.16.1 e1-TXT-639 Note

Associated Goals:

To correctly identify the medicinal product that has to be dispensed

For safety reasons

Actors: Dispenser, Dispense provider, NCPs

I.e., the medicinal product description, (e.g. paracetamol 'XXX' 500mg 12 tablets) previously translated as defined in WP3.5 'Semantic Services' and with intelligible information as described in FR05,06 and 07.

Regarding the field of 'Advice to the dispenser', as it is available in the language of country A, to avoid legal and ethical issues to the dispenser, it is RECOMMENDED to implement an option that allows the dispenser to decide, knowing that this data is available, if he wants to consult it.

3.5.2.17 e1-REQ-4551 FR14- Substitution

Tested by e1-REQ-5196 FR14 - Substitution

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

This requirement has 3 different sub_requirements:

3.5.2.17.1 e1-REQ-4677 Determination of Substitutions by HP-B

Related to e1-REQ-2089 Interpretation of the Substitution Code

The dispenser MUST be enabled to determine if in the course of translation from the medicine in country A to a medicine in country B any element of the prescription has been altered from the original one.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.17.2e1-REQ-4678 Indication of substitutions by Country B

Related to e1-REQ-2089 Interpretation of the Substitution Code

Country B must indicate to country A if substitution of Brand Name, package size or number of packages has been performed.

3.5.2.17.3e1-REQ-4679 Indication of impossible substitutions by Country A

Country A MUST indicate if a medicine (commercial product) cannot be substituted, Pharmacist MUST be aware of this when dispensing.

3.5.2.17.4e1-TXT-640 Note

Associated Goals:

Security reasons

Safety reasons

Actors: Dispenser, Dispense provider, NCPs

As the processes in each country are not in the scope of the document, pharmacist must know if the original data send by country A and received in country B is altered by country B.

Country B has to send to country A the original dispense information (i.e. without any semantic transformation) so country A can check if substitution has taken place. It is recommended to indicate if substitution has taken place by an specific field.

Some commercial products can not be substituted by legislation (normally products with a narrow therapeutic index and or release) This could be indicated by an specific field on the eP.

The issues regarding the substitution of the medicinal product are described in detail in D3.1.2, chapter 5.2.1.2

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.5.2.18 e1-REQ-4552 FR15- Dispensed medicine information sent to country A

Related to e1-REQ-3984 About the dispensed medicine data

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2083 eD to eP traceability

Related to e1-REQ-4629 epSOS DispensationService Service Interface & Functional Specification

Tested by e1-REQ-5160 FR15 - Dispensed medicine information sent to country A

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The information about the dispensed medicine event as defined in D3.1.2, chapter 6.2 MUST be sent to country A.

If there is more than one medicine dispensed, the fields related to identification of patient, dispenser and the dispensed medicine data sets MUST be provided per medicine dispensed.

Country B MUST assure the successful delivery of the dispensed medicine information to country A before country B request the 'available' prescriptions for the same patient again. This MUST be accomplished in real time and right after the medicines have been dispensed.

Country A MUST assure that the 'available' prescriptions have been updated with that information before answering country B of the successful receipt of the medicine dispensed information.

Dispensation information MAY be used by a country to automatically update internal patient data.

3.5.2.18.1 e1-TXT-641 Note

Associated Goals:

The prescription provider of country A must be informed about the dispensed medicine

Security reasons

Actors: Dispenser, Dispense provider, NCPs

In the case that the prescription contained several items, there will be a set of patient, dispenser and dispensed medicine data per item.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.19 e1-REQ-4553 FR16- Univocal relation between original prescription and medicinal product dispensed

Related to e1-REQ-1987 Relationships among Documents and/or Document Entries

Related to e1-REQ-2083 eD to eP traceability

Tested by e1-REQ-5161 FR16 - Univocal relation between original prescription and medicinal product dispensed

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The dispensed medicine dataset must contain the necessary information to allow univocal identification of the original prescription that the dispense was based on (link between dispensed medicine and prescription).

3.5.2.19.1 e1-TXT-642 Note

Associated Goals:

To update the status of the prescription

To link the dispensed information to the prescription

Actors: Prescriptionprovider and Dispenseprovider, NCPs

3.5.2.20 e1-REQ-4554 FR17- Original dispensed medicine

Related to e1-REQ-4629 epSOS DispensationService Service Interface & Functional Specification

Tested by e1-REQ-5162 FR17 - Original dispensed medicine

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Country A MUST know the original, not translated, dispensed medicine in country B, including product description and brand name, and the one in the epSOS semantic format to be able to verify the active ingredient dispensed.

3.5.2.20.1 e1-TXT-643 Note

Associated Goals:

For safety and security reasons as the brand name of the product is probably going to be changed. If the patient withdraws a different medicine and when taking it, he has adverse reaction, the country A HP will be able to diagnose based on the information on what it was originally prescribed and what the patient has actually taken

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Traceability reasons

Actors: Dispense provider, NCPs

In most cases, the same medicinal product does not exist and substituting active ingredient is out of the scope of epSOS.

3.5.2.21 e1-REQ-4600 REQ 3.3.15 eP data are not modifiable by country B

Related to e1-REQ-4585 REQ 3.3.0 Modifications to medical data received from Country-A by HP-B

Tested by e1-REQ-5197 REQ 3.3.15 eP data are not modifiable by country B

ePrescription data shall not be modified by country B.

3.5.2.22 e1-REQ-2085 eP is not a collection of patient prescriptions

Tested by e1-REQ-5198 eP is not a collection of patient prescriptions

Related to e1-REQ-4629 epSOS DispensationService Service Interface & Functional Specification

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The eP document reflects the act of prescribing, it must not be a collection of patient prescriptions.

3.5.2.23 e1-REQ-4596 REQ 3.3.11 Notification with eDispensation document

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-4629 epSOS DispensationService Service Interface & Functional Specification

Tested by e1-REQ-5199 REQ 3.3.11 Notification with eDispensation document

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

A new eDispensation document created in country B shall be transmitted to country A by a dedicated transaction.

3.5.2.24 e1-REQ-4597 REQ 3.3.12 Country A responsibility to update EHR with dispense notification

Related to e1-REQ-4629 epSOS DispensationService Service Interface & Functional Specification

Tested by e1-REQ-5200 REQ 3.3.12 Country A responsibility to update EHR with dispense notification

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Country A may update medical data within its own national infrastructure with a new eDispensation document received from country B.

3.5.2.25 e1-REQ-4671 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Tested by e1-REQ-5184 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Cross-border exchange of medical data MUST be documented in a fully traceable, reconstructable, and seamless fashion.

Cross-border exchange of medical data MUST produce a usable chain of digital evidence that enables both, the patient and his assigned DPA, to pursue, enforce, and proof any assumed or detected violation of the patient's data protection and privacy rights.

The chain of digital evidence MUST disclose the minimum of personal health data required to serve its purpose and MUST be specifically safeguarded against wrongdoing. Part of these safeguards MUST be a protocol that is not accessible to HPs.

Implications:

Audit trails SHOULD be written at both NCPs. For the purpose of data minimization NCP audit trails SHOULD not include medical data but just refer to (and safeguard) respective audit trails within HP systems.

3.5.2.25.1 e1-REQ-4555 FR20- Information Traceability

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The information describing the process and the data involved in the process MUST be retrievable. This MUST include information such as the prescriber, the exact place and time where the prescription was made, the identification of the Pharmacy where the medicine was dispensed, the dispenser that dispensed, if there was substitution, the original prescription, the translation of the prescription from country A to country B, the epsos format.

Specifically this information MUST encompass all data elements as defined by D3.1.2 chapter 6.1 and chapter 6.2.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.25.2 e1-TXT-644 Note

Associated Goals:

Security reasons

Legal reasons

Actors: Prescriber and Dispenser, Prescriptionprovider and Dispense provider, NCPs

Some of this information is not necessarily contained in the datasets exchanged between countries (as they have been considered maximum datasets) but must be able to be traced and recovered.

3.5.2.26 e1-REQ-4557 NFR01- Service availability

Synchronized with e1-REQ-3876 NFR01- Service availability

Related to e1-REQ-4908 Expected Actions

Related to e1-REQ-4918 Expected Actions

Tested by e1-REQ-5185 NFR01 - Service availability

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Each unpredictable service interruption MUST be detected as soon as possible. The origin of the failure (HP system, NCP system...) MUST be explained. It MUST be declared which systems or types of information that cannot be reached at the present time due to circumstances or technical failures. The procedure to follow MUST be specified in order to come back to a normal mode.

Instead of completely unavailability, the service MAY be degraded. This state MUST be defined and when this happens, the suitable alerts and the procedures to follow MUST be defined.

3.5.2.26.1 e1-TXT-646 Note

Associated Goals:

The epSOS service will be continuously available

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.5.2.27 e1-REQ-4558 Data Integrity

Synchronized with e1-REQ-1978 Data Integrity

Tested by e1-REQ-5186 Data Integrity

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The integrity of transmitted data MUST be preserved when information is transmitted between different entities (legally or technically defined). It must be verifiable to a data receiver that data has not been damaged, altered or (partially) lost.

3.5.2.27.1 e1-TXT-657 Note

Associated Goals:

To have secure communication means between National Contact Points

3.5.2.28 e1-REQ-4559 NFR03- Response time

Synchronized with e1-REQ-3878 NFR03- Response time

Tested by e1-REQ-5187 NFR03 - Response time

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The system MUST be able to answer to the HP in an acceptable response time.

3.5.2.28.1 e1-TXT-647 Note

Associated Goals:

Information has to travel from one country to another. An acceptable time response not only applies to the receipt of information, but also to the identification and authentication of HP and patient

The system should provide an acceptable end-to-end response time, not degrading or delaying the already existing services because the patient is waiting while the system accesses and shows the required information

The access times should be tested continually by the system to give the user some idea of what to expect

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.5.2.29 e1-REQ-4561 NFR05- Access control

Synchronized with e1-REQ-3880 NFR05- Access control

Tested by e1-REQ-5188 NFR05 - Access control

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

As authorisations involve the existence of a treatment context inside a HCPO, these treatment relationships must be justifiable on demand. The communication partners (origin, destination, and potential facilitators) MUST be known to each other with prior positive verification that all involved partners are authentic (security features to be provided by the means of an identity (subjects, actors, objects) and access management).

3.5.2.29.1 e1-TXT-648 Note

Associated Goals:

For traceability reasons

For security reasons

To assure confidentiality

For Confidentiality and integrity of medical data reasons

To align to the European Data Protection Regulations

3.5.2.30 e1-REQ-4563 Data Origin and Data Authenticity

Synchronized with e1-REQ-1984 Data Origin and Data Authenticity

Tested by e1-REQ-5189 Data Origin and Data Authenticity

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

The intended recipient of a medical data communication MUST be able to determine the originator and level of authenticity of the medical data received. Information on the identity and authenticity of the data originator that is assigned to the data or its metadata MUST NOT be altered during cross-border transfer.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.5.2.30.1 e1-TXT-655 Note

Associated Goals:

To guarantee that the issuer of the information exchanged cannot refuse that the issuance has taken place.

3.5.2.31 e1-REQ-4565 NFR09- Trust between countries

Synchronized with e1-REQ-4564 NFR09- Trust between countries

Tested by e1-REQ-5190 NFR09 - Trust between countries

Related to e1-REQ-4591 REQ 3.3.6 Secure Context Establishment

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

All the countries involved in the project are integrated into one circle of trust (technical). An agreed framework for creating trust MUST be established, encompassing processes and procedures for critical data protection, privacy and confidentiality issues as well as mechanisms for their audit. Such issues include, but are not limited to:

- Identification, authentication and authorisation mechanisms
- Security and trust mechanisms
- Recording and exchanging patient consent

3.5.2.31.1 e1-TXT-651 Note

Associated Goals:

To enable the exchange of information between countries.

To avoid having to identify all professionals and institutions from a foreign country in the country of origin. On the one hand, each HP will be unequivocally identified and authenticated in his local system and must be identified based on his/her role/profile. On the otherhand, Health Care Provider Organisation provides HP a status, a function, an authentication from which the HP trust is derived. Furthermore, Health Authorities Institutions assign and assure the status, the role, and sometimes the authentication of HP.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.32 e1-REQ-4566 NFR10- Guaranteed delivery

Synchronized with e1-REQ-3885 NFR10- Guaranteed delivery

Related to e1-REQ-4918 Expected Actions

Related to e1-REQ-4908 Expected Actions

Tested by e1-REQ-5191 NFR10 - Guaranteed delivery

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

When information is sent from one country to another, it MUST be assured that the information has been properly received by the user in the receiver country.

3.5.2.32.1 e1-TXT-652 Note

Associated Goals:

security reasons

to check that the ePrescription service has been properly completed

3.5.2.33 e1-REQ-4567 NFR11- Single session

Synchronized with e1-REQ-3886 NFR11- Single session

Tested by e1-REQ-5192 NFR11 - Single session

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

In order to avoid fraud, it MUST NOT possible to open more than one session for the patient at a time.

3.5.2.33.1 e1-TXT-653 Note

Associated Goals:

For security reasons

To avoid a patient withdrawing the same medicine at the exact time from different pharmacies

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.34 e1-REQ-4568 NFR12- Supervision services

Synchronized with e1-REQ-3887 NFR12- Supervision services

Tested by e1-REQ-5193 NFR12 - Supervision services

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

A service MUST be put in place to detect all the technical exceptions and to check and monitor the performance of the service (time response, communications...).

3.5.2.34.1 e1-TXT-654 Note

Associated Goals:

To assure the availability and to avoid degradation of the service

3.5.2.35 e1-FLD-129 Information Model

3.5.2.35.1 e1-REQ-4626 Information Model: Patient Summary & ePrescription

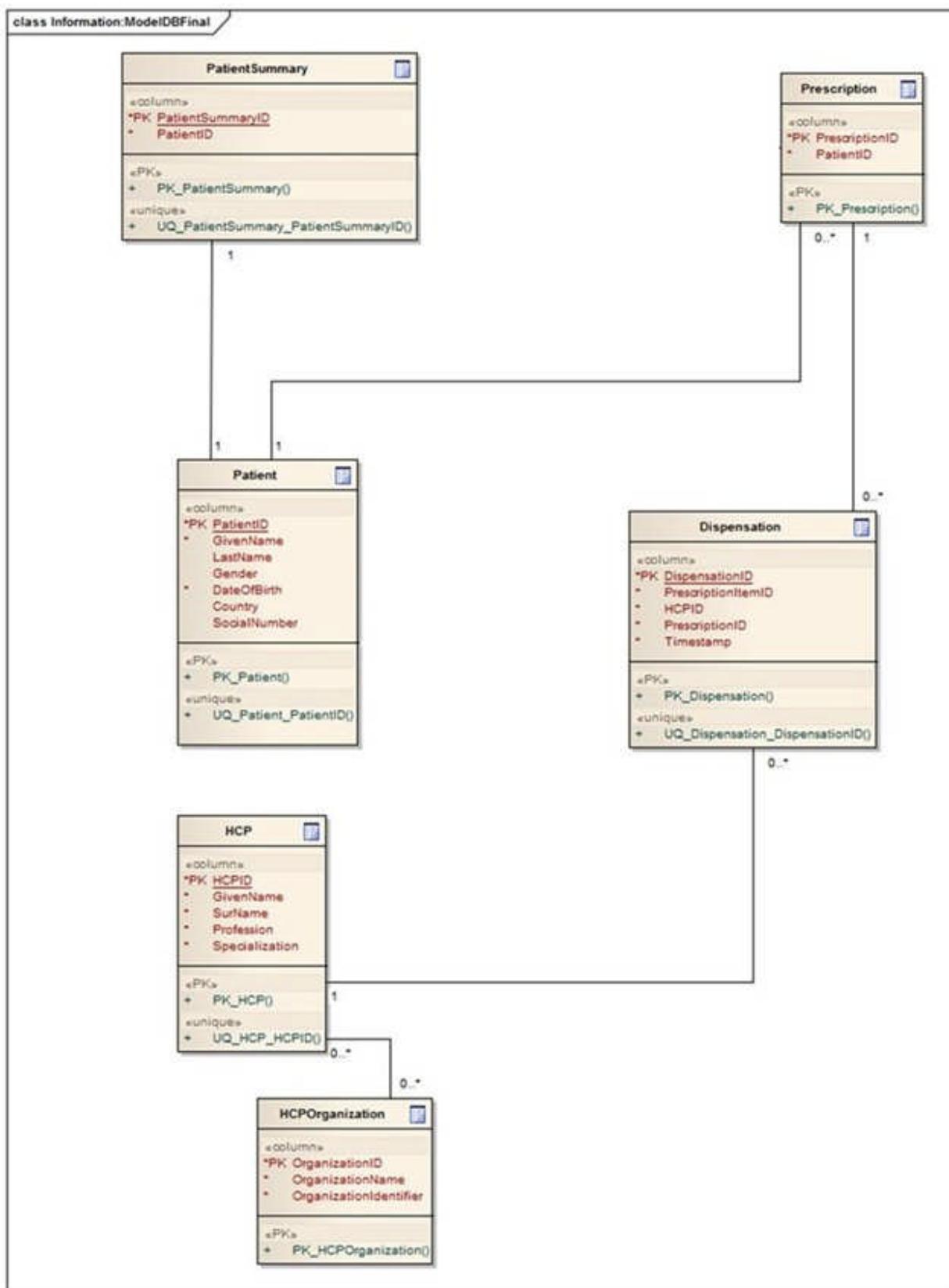
Related to e1-REQ-3984 About the dispensed medicine data

Related to e1-REQ-1670 About the prescription data in the ePrescription

Synchronized with e1-REQ-4624 Information Model: Patient Summary & ePrescription

Related to e1-REQ-2096 eD template conformance

Related to e1-REQ-2093 eP template conformance



	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Health Professional (HP)

A health care professional is a physician participating in epSOS identifiable by its unique id. It is affiliated to zero or more health care professional organizations, depending on national legislation.

The HP contains information as defined in D3.1.2. A HP is related to 0..n HCPOs and is associated with 1..n Healthcare Professional Addresses.

Health Care Professional Organization (HCPO)

A Health Care Professional Organization is a logical entity within the national environment known to the NCP and uniquely identifiable by its id.

The HCPO object contains information defined in D3.1.2. An HCPO is related to 1..n HPs. At any given time in the context of an epSOS transaction, an HP is associated with only one HCPO.

Patient

A patient is an individual person participating in epSOS by giving permission (prior consent) in his home community to process his/her medical data to a foreign participating nation.

The Patient object contains information defined in D3.1.2. A patient is related to 1..1 PS, 0..* ePs and 0..* eDispenses.

[3.5.2.35.2 e1-REQ-4627 State Model: ePrescription](#)

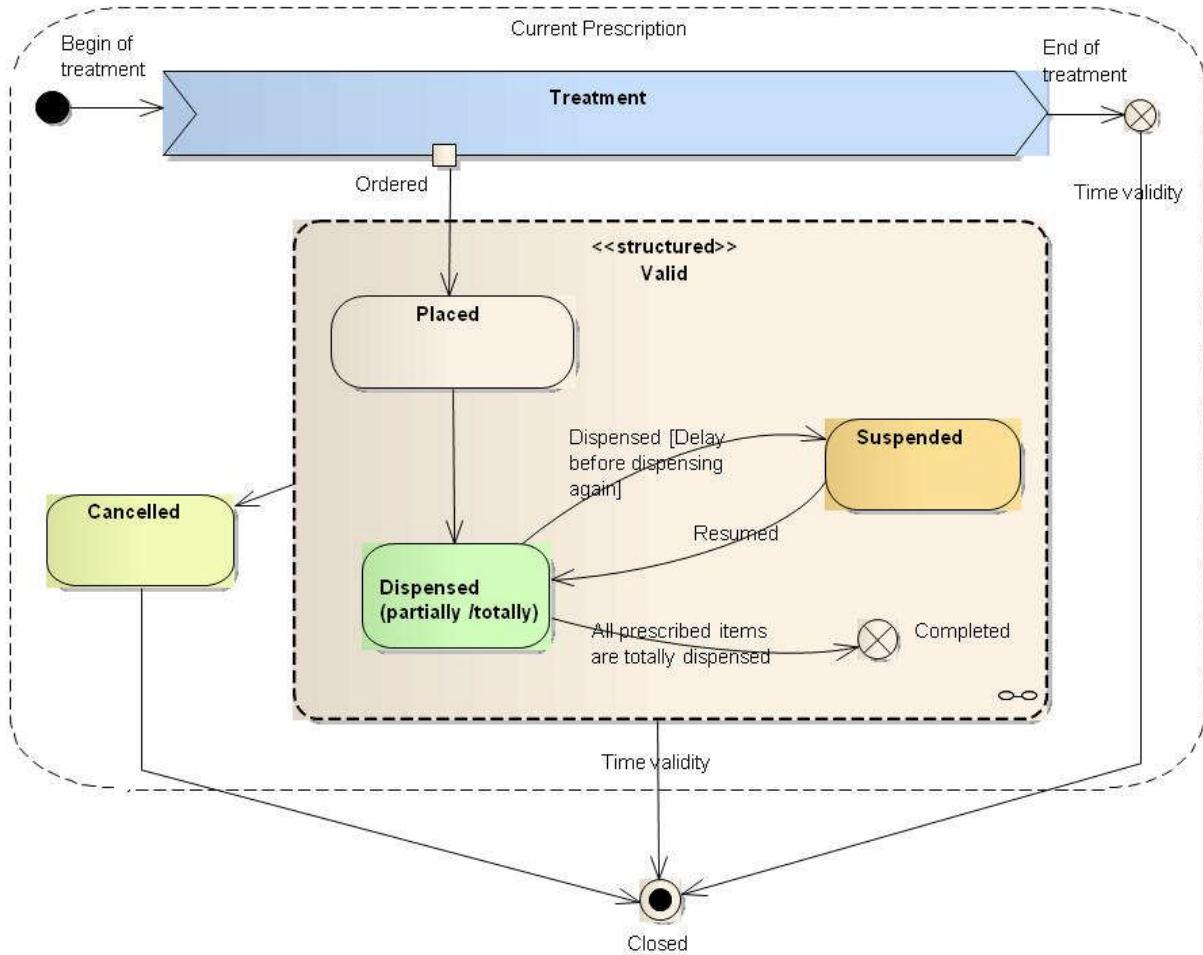
The eP object contains information about the medicine prescribed in country A. The status management of the eP is an internal PN affair (i.e. it may differ from country to country) and D3.1.2 does not give specifications for this topic. The minimum basic status is "Available" or "Not Available" as presented for the Patient Summary.

The figure below shows a suggested lifecycle for an eP. When looking at the lifecycle the following states can be reached by an eP:

1. Ordered: This state is reached when the prescriber has written the eP and the eP is included in the patient's electronic health record (EHR).
2. Placed: This state is reached when the ordered eP has been recorded into the national/regional eP service and is now ready to be accessed by the dispenser.
3. Cancelled: This state is reached if the eP is invalidated before dispensed completely.
4. Suspended: If an eP can be dispensed more than one time and requires a certain time span between dispensations, the eP assumes the state Suspended in this time. It reaches the state Partially dispensed when the eP becomes available again.
5. Partially Dispensed: If a single ePrescription contains multiple items -or items which can be multiply dispensed - it reaches this state if the eP is not dispensed completely.
6. Completed: This state is reached when all ePrescription items have been fully dispensed.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

7. Closed: This state is reached if the eP loses its validity before it has been fully dispensed (e.g. the eP's time validity has run out, or the patient has withdrawn consent).



	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.5.2.35.3 e1-REQ-4630 State Model: eDispensation

In epSOS the event of a patient's eDispense is handled via a notification message from country B to country A. Country A decides how to handle the eDispense event.

3.5.2.35.4 e1-TXT-727 Note

Since an ePrescription may contain multiple ePrescription items, it must be possible to allow multiple eDispenses for one ePrescription.

There are two ways for the NCP to handle multiple eDispenses (for details see D3.4.2):

If not all eP Items have been dispensed as seen in the notification, generate a new eP containing only the non-dispensed medicines. This is a task of the HP. Nevertheless, according to every PN legislation, this option may be implemented at the NCP level.

If not all ePrescription Items have been dispensed, return the original ePrescription again and raise an error if a notification is received on an already dispensed medicine. This requires that the pharmacists MUST wait for the result of the notification before the pharmacist can dispense the medicine to the patient.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

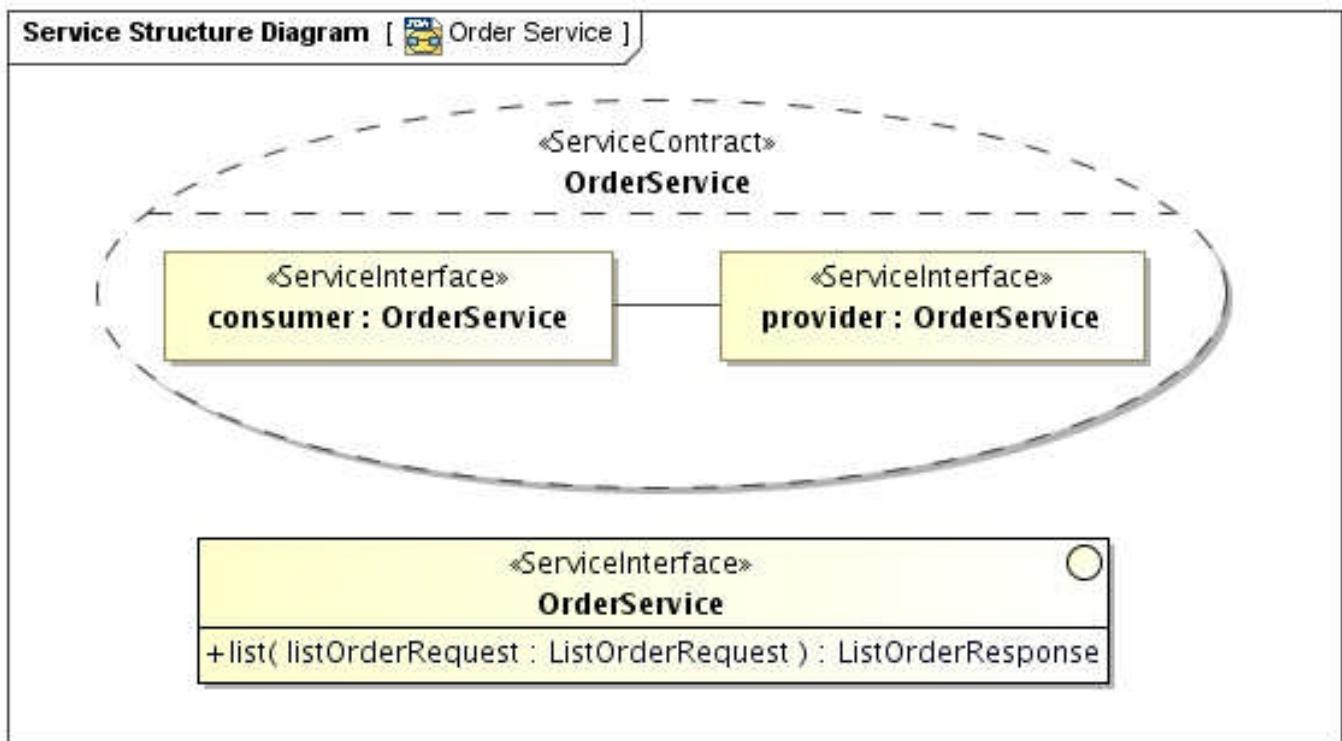
3.5.2.36 e1-FLD-130 Computational Dimension

3.5.2.36.1 e1-REQ-4628 epSOS OrderService Service Interface & Functional Specification

Related to e1-REQ-4549 FR12- Original prescription

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Related to e1-REQ-4842 epSOS OrderService Service Interface & Functional Specification



Operation list()

Description Obtain the epSOS-encoded, available ePrescriptions of the identified patient

Requestor Consuming Gateway at NCP-B

Input ListOrderRequest

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Message	Body	Identifier of the patient whose available ePrescriptions are requested
	Security Token	X.509 Gateway Certificate
		epSOS HCP Identity Assertion epSOS Treatment Relationship Confirmation Assertion
Output Message in successful Case	ListOrderResponse	
	Body	<p>List of epSOS-encoded ePrescriptions</p> <p>original ePrescriptions (e.g. PDF/A encoded) of the identified patient</p> <p>information on the status of this list (e. g. more ePrescriptions are available but NCP-A was unable to transform these into the epSOS pivot format)</p>
	Security Token	X.509 Gateway Certificate
Precondition of success scenario		<p>The requestor is able to locate the service provider</p> <p>The certificate of the NCP-A gateway is available to the requestor.</p> <p>The requestor is able to verify the certificate of the NCP-A gateway.</p> <p>The NCP-A gateway is able to verify the requestor's certificate.</p> <p>An HCP identity assertion has been issued by NCP-B and is available to the requestor</p> <p>The NCP-A gateway is able to verify the validity of the HCP identity assertion</p> <p>NCP-A and NCP-B agreed on a common ID for referencing to the patient</p> <p>An TRC assertion has been issued by NCP-B and is available to the</p>

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

requestor

The NCP-A gateway is able to verify the validity of the TRC assertion

Main success scenario	Actions of the epSOS Order Service provider: validate the message signature verify HCP identity assertion and TRC assertion extract the patient ID from the message body verify that the patient has given consent to epSOS and that the consent is valid retrieve the patient's available ePrescriptions enforce national security policy and (if available) patient privacy policy verify authenticity and integrity of the ePrescriptions transform ePrescriptions into epSOS pivot format (if requested and needed) render PDF from the source document (if requested and needed) sign the response message and send it to the requestor
Fault	Preconditions for a success scenario are not given Requestor has insufficient rights to access the patient's ePrescriptions No patient summary is available for the identified patient The patient summary cannot be provided in the requested encoding Temporary failure (e.g. authenticity verification cannot be performed due to a PKI failure)
Warning	Country A allows for data hiding; a respective disclaimer SHOULD be shown to the HP Mandatory fields have been nullified for some of the provided ePrescriptions (minimum dataset is not fully provided); the HP MUST

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

additionaly consider the source coded document

More ePrescriptions MAY be available but are not accessible

The computation of the CDA encoded ePrescription documents was not approved by an HP; a respective disclaimer MUST be shown to the HP

Partial Delivery: It must be assessed if partial delivery conditions could be signaled on the content level (within the documents) instead of transmitting such information on the transaction level.

3.5.2.36.2 e1-REQ-4629 epSOS DispensationService Service Interface & Functional Specification

Related to e1-REQ-2085 eP is not a collection of patient prescriptions

Related to e1-REQ-4552 FR15- Dispensed medicine information sent to country A

Related to e1-REQ-4554 FR17- Original dispensed medicine

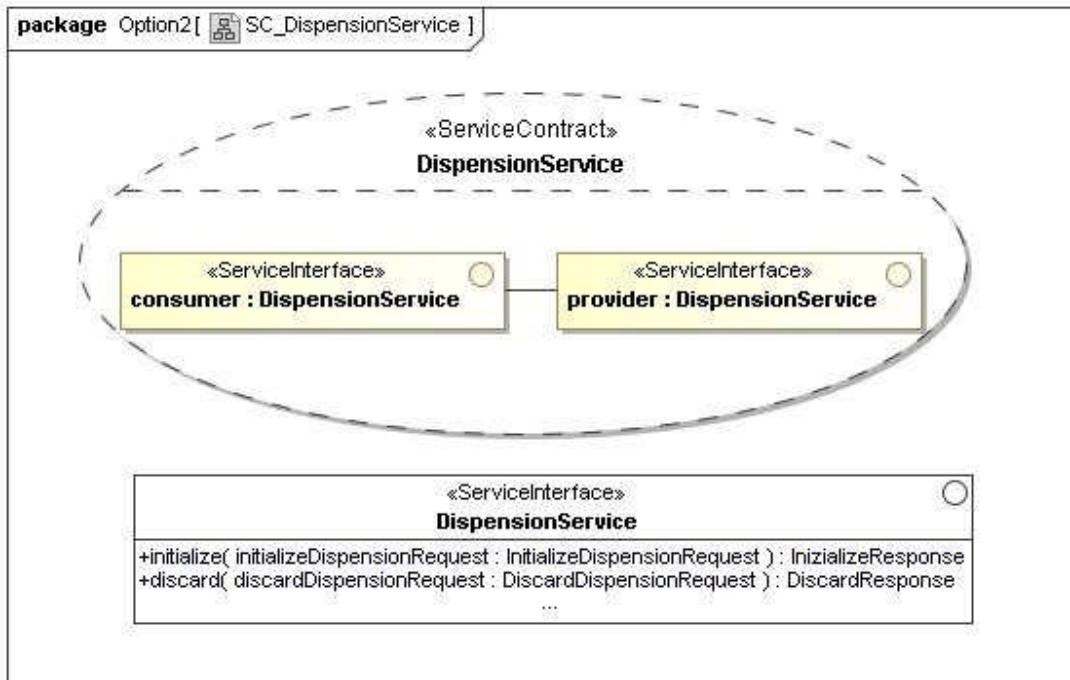
Related to e1-REQ-4596 REQ 3.3.11 Notification with eDispensation document

Related to e1-REQ-4597 REQ 3.3.12 Country A responsibility to update EHR with dispense notification

Related to e1-REQ-4458 UC.eP.1 Medicine already prescribed in country A

Related to e1-REQ-4843 epSOS DispensationService Service Interface & Functional Specification

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



Operation	initialize()
Description	Notify the patient's country of affiliation on a successful dispensation of an ePrescription
Requestor	Consuming Gateway at NCP-B
Input Message	initializeDispensationRequest
Body	eDispensation dataset as defined by D3.5.2. This dataset contains a reference to the dispensed ePrescription document.
Security Token	X.509 Gateway Certificate
	epSOS HCP Identity Assertion epSOS Treatment Relationship Confirmation Assertion

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Output Message in successful Case	initializeDispensationResponse Body empty Security Token X.509 Gateway Certificate
Precondition of success scenario	<p>The requestor is able to locate the service provider</p> <p>The certificate of the NCP-A gateway is available to the requestor.</p> <p>The requestor is able to verify the certificate of the NCP-A gateway.</p> <p>The NCP-A gateway is able to verify the requestor's certificate.</p> <p>An HCP identity assertion has been issued by NCP-B and is available to the requestor</p> <p>The NCP-A gateway is able to verify the validity of the HCP identity assertion</p> <p>NCP-A and NCP-B agreed on a common ID for referencing to the patient</p> <p>An TRC assertion has been issued by NCP-B and is available to the requestor</p> <p>The NCP-A gateway is able to verify the validity of the TRC assertion</p>
Main success scenario	<p>Actions of the epSOS Dispensation Service provider:</p> <p>validate the message signature</p> <p>verify HCP identity assertion and TRC assertion</p> <p>extract the ePrescription ID from the message body</p> <p>verify that the patient has given consent to epSOS and that the consent is valid</p> <p>enforce national security policy and (if available) patient privacy policy</p> <p>perform activities acc. to country-A dispensation regulations</p> <p>sign the response message and send it to the requestor</p>

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Operation	discard()	
Description	Notify the patient's country of affiliation on an erroneous creation of an eDispensation	
Requestor	Consuming Gateway at NCP-B	
Input Message	discardDispensationRequest	
	Body	eDispensation dataset as defined by D3.5.2. This dataset contains a reference to the dispensed ePrescription document.
	Security Token	X.509 Gateway Certificate
		epSOS HCP Identity Assertion
Output Message in successful Case	discardDispensationResponse (conforms to response message; see section 4.2)	
	Body	empty
	Security Token	X.509 Gateway Certificate
Precondition of success scenario	<p>The requestor is able to locate the service provider</p> <p>The certificate of the NCP-A gateway is available to the requestor.</p> <p>The requestor is able to verify the certificate of the NCP-A gateway.</p> <p>The NCP-A gateway is able to verify the requestor's certificate.</p> <p>An HCP identity assertion has been issued by NCP-B and is available to the requestor</p> <p>The NCP-A gateway is able to verify the validity of the HCP identity assertion</p>	
Main success scenario	Actions of the epSOS Dispensation Service provider: validate the message signature	

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

- verify HCP identity assertion assertion
 - extract the ePrescription ID from the message body
 - discover the patient the ePrescription was issued for
 - verify that the patient has given consent to epSOS and that the consent is valid
 - enforce national security policy and (if available) patient privacy policy
 - verify that is was the requestor who previously dispensed the ePrescription
 - perform activities acc. to country-A dispensation regulations
 - sign the response message and send it to the requestor
-

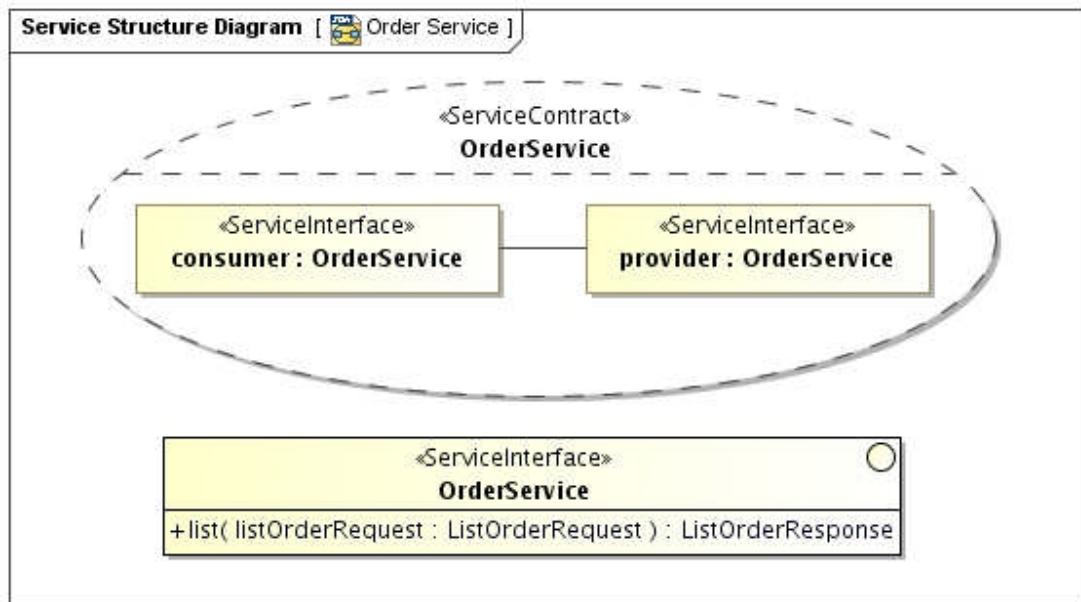
	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.2.36.3 e1-REQ-4842 epSOS OrderService Service Interface & Functional Specification

Related to e1-REQ-4628 epSOS OrderService Service Interface & Functional Specification

Related to e1-REQ-4841 General Considerations for Successful Service Operations

Related to e1-REQ-4903 epSOS Order Service Message Specification



Operation: list

Operation list()

Description Obtain the epSOS-encoded, available ePrescriptions of the identified patient

Requestor Consuming Gateway at NCP-B (service consumer at the country of care)

Input
Message ListOrderRequest

Body	(1) Identifier of the patient whose available ePrescriptions are requested (2) Optional: epSOS CDA template qualifier (pivot and/or source coded documents). If no
------	---

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

template qualifier is given the service provider MUST respond with all available encodings of the requested documents.

Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion [O]
Output Message in successful Case	ListOrderResponse
Body	(1) List of (1a) epSOS-encoded ePrescriptions and/or (1b) source coded ePrescriptions (acc. to requested format) Of the identified patient
Security Token	[PT] X.509 NCP-A service certificate
Precondition of success scenario	In addition to the requirements stated in e1-REQ-4841 the following preconditions MUST be met for successful processing: Service consumer and service provider share a common identifier for the patient The patient has given consent to the use of epSOS A treatment relationship exists between the patient and the requesting HP and the attesting assertion can be verified by the service provider The HP is authorised to access the requested data
Main success scenario	Actions of the epSOS Order Service provider: Validate the authenticity of the service consumer Verify HCP identity assertion and TRC assertion Verify that the patient has given valid consent to epSOS and that the consent applies to the current usage scenario Retrieve patient's available prescriptions source documents

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Enforce national security policy and (if available) patient privacy policy

Verify authenticity and integrity of available prescriptions

Transform ePrescriptions into epSOS pivot format (if requested and needed) and write a respective audit trail entry

Render PDF from source document (if requested and needed)

Apply epSOS protection means to the response message and send it to the requestor

Fault Conditions	<p>Preconditions for a success scenario are not met</p> <hr/> <p>Requestor has insufficient rights to access the patient's ePrescriptions</p> <hr/> <p>No consent for ePrescription sharing is registered for the identified patient</p> <hr/> <p>A (referenced) ePrescription cannot be provided in the requested encoding</p> <hr/> <p>Temporary failure (e. g. authenticity verification cannot be performed due to a PKI failure)</p>
------------------	---

[1] Even though the minimum dataset is considered as mandatory, there MAY be situations where country A MAY nevertheless wish to even transmit a document with parts not being translated in order to signal the existence of more data that can be accessed by requesting the respective document without pivot translation (e.g. in cases where the affected countries share the same language)

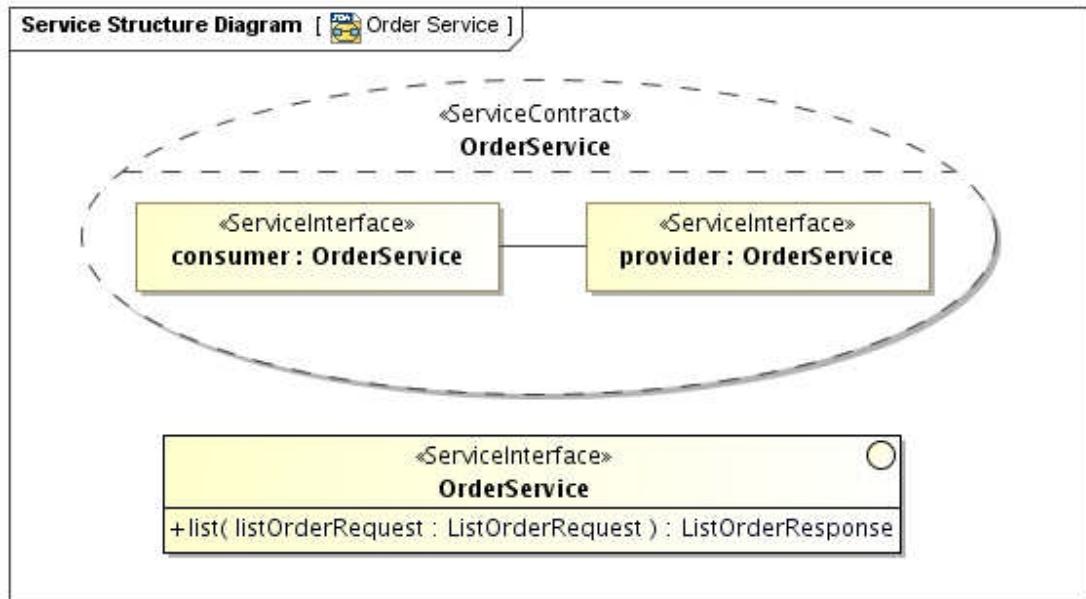
3.5.2.36.4 e1-REQ-4843 epSOS DispensationService Service Interface & Functional Specification

Related to e1-REQ-4629 epSOS DispensationService Service Interface & Functional Specification

Related to e1-REQ-4841 General Considerations for Successful Service Operations

Related to e1-REQ-4914 epSOS Dispensation Service Message Specification

 European Patients Smart Open Services	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013



Operation: initialize

Operation	initialize()
Description	Notify the patient's country of affiliation on a successful dispensation of an ePrescription
Requestor	Consuming Gateway at NCP-B (service consumer at the country of care)
Input Message	<p>initializeDispensationRequest</p> <p>Body</p> <p>(1) epSOS coded eDispensation documents as defined by epSOS D3.5.2.</p> <p>(2) source coded dispensation data</p> <p>The body MUST contain at least one epSOS pivot coded dispensation document (1). It MUST contain at least one source coded document (2). There MUST be a 1:1 association among provided source coded documents and</p>

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

epSOS coded eDispensation documents.

Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion [O]
Output Message in successful Case	initializeDispensationResponse
Body	(1) Success indicator
Security Token	[PT] X.509 NCP-A service certificate
Precondition of success scenario	<p>In addition to the requirements stated in e1-REQ-4841 the following preconditions MUST be met for successful processing:</p> <p>Service consumer and service provider share a common identifier for the patient</p> <p>The patient has given consent to the use of epSOS</p> <p>The service consumer has previously retrieved the list of the patient's available ePrescriptions</p> <p>All available ePrescriptions for the identified patient are accessible for NCP-A and the provided eDispensation data relates to these ePrescriptions</p> <p>A treatment relationship exists between the patient and the requesting HP and the attesting assertion can be verified by the service provider</p> <p>The HP is authorised to dispense medication for the patient</p>
Main success scenario	<p>Actions of the epSOS Dispensation Service provider:</p> <p>Validate the authenticity of the service consumer</p> <p>Verify HCP identity assertion and TRC assertion</p> <p>Verify that the patient has given consent to epSOS and that the consent is valid</p> <p>Enforce national security policy and (if available) patient privacy policy</p>

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Verify that all dispensation information is provided and that dispensation data is properly coded

Retrieve patient's available prescriptions and verify that each dispensation item matches with a prescribed item

Process the dispensation information

Apply epSOS security measures to the success indicator and send it to the requestor

Fault Conditions	<p>Preconditions for a success scenario are not met</p> <hr/> <p>The requesting HP has insufficient rights to dispense the identified patient's ePrescriptions</p> <hr/> <p>One or more of the provided dispensation items do not relate to available ePrescriptions of the identified patient</p> <hr/> <p>The ePrescription that is referred to by an eDispensation has already been dispensed.</p> <hr/> <p>No consent for ePrescription sharing and dispensing is registered for the identified patient</p> <hr/> <p>The eDispensation data is not provided in all mandatory encodings</p> <hr/> <p>Temporary failure (e.g. verification of a signature cannot be performed due to a PKI failure)</p>
------------------	---

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Operation: discard

Operation	Discard()	
Description	Notify the patient's country of affiliation on an erroneous eDispensation notification, in order to allow it to roll back any changes made on its internal data that were triggered by the erroneous notification	
Requestor	Consuming Gateway at NCP-B (service consumer at the country of care)	
Input Message	discardDispensationRequest	
	Body	(1) Identifier of the eDispensation document that is to be discarded
	Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion
Output Message in successful Case	discardDispensationResponse	
	Body	Success indicator
	Security Token	[PT] X.509 NCP-A service certificate
Precondition of success scenario	In addition to the requirements stated in e1-REQ-4841 the following preconditions MUST be met for successful processing: Service consumer and service provider share a common identifier for the patient The service consumer has previously retrieved the list of the patient's available ePre-scriptions and dispensed the identified medicine	
Main success scenario	Actions of the epSOS Dispensation Service provider: Validate the authenticity of the service consumer Verify HCP identity assertion Extract the dispensed item id from the message body and ensure that	

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

this item was previously dispensed by the identified HP

Enforce national security policy and (if available) patient privacy policy

Rewind the dispensation

Sign the success notification and send it to the requestor

Fault Conditions	<p>Preconditions for a success scenario are not met</p> <hr/> <p>The HP has insufficient rights to process the patient's ePrescription data</p> <hr/> <p>The HP was not the original dispenser of the identified medication item</p> <hr/> <p>The identified item had not been dispensed previously</p> <hr/> <p>Temporary failure (e.g. service provider is temporarily unable to access an internal service)</p>
------------------	--

3.5.2.36.5 e1-TXT-734 Note

Even though the minimum dataset is considered as mandatory, there MAY be situations where country A MAY nevertheless wish to even transmit a document with parts not being translated in order to signal the existence of more data that can be accessed by requesting the respective document without pivot translation (e.g. in cases where the affected countries share the same language).

The respective discard() operation is introduced in D3.3.2. It is solely motivated by the requirement that epSOS in any case MUST protect the integrity of existing data. For this reason it is not part of the functional requirements as expressed in D3.1.2.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3 e1-FLD-81 Implementable Perspective

3.5.3.1 e1-FLD-166 Information Dimension

3.5.3.1.1 e1-REQ-2093 eP template conformance

Related to e1-REQ-4546 FR09- Prescription presentation

Related to e1-REQ-4550 FR13- Identification of the medicinal product

Related to e1-REQ-4626 Information Model: Patient Summary & ePrescription

Related to e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-2074 CDA conformance

Related to e1-REQ-2076 Coded elements attributes optionality

Related to e1-REQ-2080 Consumer capabilities (epSOS PDF)

Related to e1-REQ-2079 Document Instance Identifier

Related to e1-REQ-2091 Element <translation>

Related to e1-REQ-2075 epSOS CDA Recipient Responsibilities

Related to e1-REQ-2097 epSOS pdf conformance

Related to e1-REQ-2082 epSOS PDF – epSOS pivot link

Related to e1-REQ-2081 Implementable Original document identification

Related to e1-REQ-2078 Link between coded elements and text

Related to e1-REQ-3894 Links among documents

Related to e1-REQ-2090 Recording of transcoded/translation data

Related to e1-REQ-2092 Reference coded system used in Country A

Related to e1-REQ-2077 Valorization of displayName

epSOS ePrescription SHALL be conformant with the template 1.3.6.1.4.1.12559.11.10.1.3.1.1.1 specification according to D3.9.1 Appendix B1.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3.1.2 e1-REQ-2096 eD template conformance

Related to e1-REQ-4552 FR15- Dispensed medicine information sent to country A

Related to e1-REQ-4626 Information Model: Patient Summary & ePrescription

Related to e1-REQ-4596 REQ 3.3.11 Notification with eDispensation document

Related to e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-2074 CDA conformance

Related to e1-REQ-2076 Coded elements attributes optionality

Related to e1-REQ-2080 Consumer capabilities (epSOS PDF)

Related to e1-REQ-2079 Document Instance Identifier

Related to e1-REQ-2091 Element <translation>

Related to e1-REQ-2075 epSOS CDA Recipient Responsibilities

Related to e1-REQ-2097 epSOS pdf conformance

Related to e1-REQ-2082 epSOS PDF – epSOS pivot link

Related to e1-REQ-2081 Implementable Original document identification

Related to e1-REQ-2078 Link between coded elements and text

Related to e1-REQ-3894 Links among documents

Related to e1-REQ-2090 Recording of transcoded/translation data

Related to e1-REQ-2092 Reference coded system used in Country A

Related to e1-REQ-2077 Valorization of displayName

epSOS eDispensation SHALL be conformant with the template1.3.6.1.4.1.12559.11.10.1.3.1.1.2 specifications according to D3.9.1 Appendix B1.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.5.3.1.3 e1-REQ-4880 epSOS ePrescription & eDispensation Documents and Codes

epSOS Consumer Document	Display Name	Coding Scheme	Node Representation
eDispensation	eDispensation	2.16.840.1.113883.6.1	60593-1
ePrescription	ePrescription	2.16.840.1.113883.6.1	57833-6

3.5.3.1.4 e1-REQ-2083 eD to eP traceability

Related to e1-REQ-4552 FR15- Dispensed medicine information sent to country A

Related to e1-REQ-4553 FR16- Univocal relation between original prescription and medicinal product dispensed

Countries shall be enabled to trace back from the eD what is the prescription dispensed, and for each dispensed item what is the prescription item supplied.

3.5.3.1.4.1 e1-REQ-2084 Mechanism facilitating eD to eP traceability

The prescription ID and prescription item ID must be globally unique. In countries where there can be only one item per prescription, the prescription item ID must be the same as the prescription ID.

The main mechanism for handling the eD and eP linkage must be by means of the prescription item ID that can be used by the prescribing system or provider to identify the prescription to which it belongs. (see D3.9.1 Appendix B1 section 12.1.3.4.8 Related prescription item).

Moreover the eD document SHALL refer the prescription ID using the InFulfillmentOf relationship. The target order.id attribute must not be the identifier of the document instance, but that of the prescription (as order).

3.5.3.1.5 e1-REQ-2086 eP has a human author (prescriber)

eP as a result of a clinical act, and independently the way it has been generated, shall always have a well-defined human prescriber as document author.

3.5.3.1.6 e1-REQ-2087 eD document the dispensation of a single eP

The eD document shall reflect the act of dispensing medications belonging to a well-defined eP document.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.5.3.1.6.1 e1-TXT-284 Example

Example: The patient has prescription from his general practitioner (GP) for high blood pressure and asthma (prescribed at the same time), and a prescription for migraines from a neurologist - three medications altogether. Country A shall present these as two eP documents with one section each, one document for the medication prescribed by the GP, the other for the medication prescribed by the neurologist.

In Country B, the patient may need two of the three to be filled - the high blood pressure and the migraine medicine. Even if they are filled by the same pharmacist at the same time Country B shall create one eD document for each eP dispensed.

3.5.3.1.7 e1-REQ-2088 Prescription Item ID

The following must be true for the prescription item ID:

The prescription item ID must be globally unique

In countries where there can be only one item per prescription, the prescription item ID must be the same as the prescription ID

The prescription item ID can be used by the prescribing system or provider to identify the prescription to which it belongs. This provides the link from the dispensed medicine to the prescription (see D3.9.1 Appendix B1 section 12.1.3.4.8 Related prescription item).

3.5.3.1.8 e1-REQ-2089 Interpretation of the Substitution Code

Related to e1-REQ-4677 Determination of Substitutions by HP-B

Related to e1-REQ-4678 Indication of substitutions by Country B

Within the epSOS-I scope the "N" code shall be interpreted as No substitution allowed excepting for the Package Size.

The presence of any other code that is not "N", or the absence of the substitution instructions, shall mean that also the brand name (as well as the Package Size) can be changed.

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version: 1.0
D5.2.3	Date: 31/01/2013

3.5.3.1.9 e1-FLD-174 epSOS Order Service

3.5.3.1.9.1 e1-REQ-4900 Request Message

The list() request MUST be initiated by an HP in the country of care for retrieving the available ePrescription documents of an identified patient. The respective request message builds upon the IHE XCF Cross-Gateway Fetch request message.

The element that encapsulates the query parameters MUST be used as follows for epSOS:

Element Name	epSOS Usage Convention
ResponseOption/@returnComposedObjects	MUST be "true"
ResponseOption/@returnType	MUST be "LeafClassWithRepositoryItem"
AdhocQuery	Container for holding the ebML stored query arguments. All arguments MUST be encoded as query slots (see table below).
AdhocQuery@id	MUST be "urn:uuid:f2072993-9478-41df-a603-8f016706efe8" which indicates a Fetch (which is an adaption of the findDocuments Query as defined in ITI TF-2a:3.18.1, August 2009)

Only synchronous web services exchange MUST be used. The *XDS Affinity Domain Option* only applies to the national environment. Therefore it MUST NOT be used for NCP-2-NCP message exchange.

Stored query argument slots MUST be defined for the patient identifier and the document class code. The document format code and the document type code MAY be given. Other argument slots than the ones listed below MUST be ignored by the service provider and SHOULD NOT be issued by the service consumer.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Slot Name	Opt	Slot Value
\$XDSDocumentEntryPatientId	R	Equals to the patient identifier that was provided by the epSOS Identification Service (encoded as HL7 v3 II data type)
\$XDSDocumentEntryStatus	R	Only approved documents MUST be returned: 'urn:oasis:names:tc:ebxml-regrep: StatusType:Approved'
\$XDSDocumentEntryClassCode	R	ePrescription LOINC code ("57833-6") coded according to specification in ITI TF-2a: 3.18.4.1.2.3.4 Coding of Code/Code-Scheme. As classification scheme 2.16.840.1.113883.6.1 MUST be used: '57833-6^^2.16.840.1.113883.6.1'
\$XDSDocumentEntryTypeCode	O	ePrescription LOINC code ("57833-6") coded according to specification in ITI TF-2a: 3.18.4.1.2.3.4 Coding of Code/Code-Scheme. As classification scheme 2.16.840.1.113883.6.1 MUST be used: '57833-6^^2.16.840.1.113883.6.1'
\$XDSDocumentEntryFormatCode	O	Format qualifier as defined in table 1C of epSOS D3.5.2C; see table below for details on applying these codes to the retrieval of a patient's available ePrescriptions. Only encodings of ePrescription documents that comply to the requested format code will be returned by the service provider. If this stored query slot is omitted, the service provider MUST respond with all available encodings.

For the document format only the format codes defined in epSOS D3.5.2C and listed in the following table MUST be used.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Document Format	Format Code	Document content
epSOS pivot coded ePrescription	urn:epSOS:ep:pre:2010	HL7 CDA document acc. epSOS D3.5.2C. The patient's country of affiliation MUST be able to provide the patient's available ePrescriptions in this format.
PDF/A source coded document	urn:ihe:iti:xds-sd:pdf:2008	CDA-enveloped PDF/A encoding of the original document without any semantic transformation. The patient's country of affiliation MUST be able to provide the patient's available ePrescriptions in this format.

3.5.3.1.9.2 e1-REQ-4901 Response Message (Full Success Scenario)

Related to e1-REQ-4908 Expected Actions

Depending on the requested format code the epSOS list() response contains the epSOS pivot encoded ePrescription documents, the PDF/A source coded ePrescription documents of the identified patient or both sets of documents. If both encodings are provided, a 1:1 association between any source coded PDF document and its derived epSOS pivot CDA coded document MUST be given.

The respective message builds upon to the IHE XCA Cross-Gateway Fetch response and Cross-Gateway Fetch Response messages, by creating a new combined QueryRetrieve-alike message[1]. The fields defined for the epSOS Order Service ListResponse message MUST be used as follows:

Element Name	epSOS Usage Convention
query:AdhocQueryResponse	Response message acc to IHE XCF Cross-Gateway Fetch response message IHE XCF
@status	For the full success scenario the response status MUST be set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" or "urn:ihe:iti:2007:ResponseStatusType:PartialSuccess"

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

	(for details see table below)
..../rs:RegistryErrorList	In case that a warning is given by the service provider, this element holds the respective warning codes and messages. It must be used acc. to section 4.1.13 of IHE ITI TF 3, October 2008.
..../rim:RegistryObjectList	This element MUST be provided for the full success scenario. It MUST at least contain one child <rim:ExtrinsicObject> element.
.../..../rim:ExtrinsicObject	For each instance of a ePrescription document a <rim:ExtrinsicObject> element MUST be provided. Each <rim:ExtrinsicObject> element is described and classified by metadata acc. to the table below.
....../..../rimext:Document	This element MUST appear as the last element child of an <rim:ExtrinsicObject> element. It may appear zero or one times. This element contains the base 64 encoded content of the document. The document contents are associated with the DocumentEntry (ExtrinsicObject) metadata by the fact that it is nested inside it within the XML. The base64 encoded document content MAY be encrypted. How encryption is applied and how the encryption key is negotiated should be subject to an additional specification on advanced security safeguards.

Each provided ePrescription document and each of its encodings (epSOS pivot and/or source coded PDF) MUST be further classified by metadata. The following table lists the usage conventions that have to be followed for the epSOS Order Service response message. If not stated otherwise the classification schemes as defined in section 4.3.1.2 of IHE ITI TF 3 October 2008 MUST be used. If no restrictions on metadata values are given, the metadata elements MUST be used as per IHE XCF.

Metadata (ebRIM names)	Binding	epSOS Opt.	epSOS usage convention
status	Attribute	R	MUST be "urn:oasis:names:tc:ebxml-regrep>StatusType:Approved"

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

MimeType	Attribute	R	MUST be “text/xml” for both epSOS pivot CDA and CDA-wrapped PDF
Name	Main	R	MAY be empty. MUST be ignored by the service consumer.
Description	Main	O	MAY be empty. MUST be ignored by the service consumer.
VersionInfo	Main	R	MUST be “1”
creationTime	rim:Slot	O	MAY be omitted by the service provider and MAY be ignored by the service consumer. If given, the value MUST be encoded as HL7 v2 Date Time “YYYY[MM[DD[hh[mm[ss]]]]]”
Hash	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.
languageCode	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.
repositoryUniqueld	rim:Slot	O	MAY be omitted by the service provider and MAY be processed by the service consumer in an IHE-compatible NI-scenario.
serviceStartTime serviceEndTime	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.
Size	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

sourcePatientId	rim:Slot	R	MUST contain the same value as XDSDocumentEntry.PatientId (see below).
sourcePatientInfo	rim:Slot	X	MUST NOT be used. Future versions of epSOS MAY define different protection levels for metadata and documents. Therefore all metadata elements that might carry medical or social information MUST be omitted.
classCode	Classification	R	ePrescription LOINC code ("57833-6"). As classification scheme "urn:oid:2.16.840.1.113883.6.1" MUST be used
eventCodeList	Classification	X	MUST NOT be used. Future versions of epSOS MAY define different protection levels for metadata and documents. Therefore all metadata elements that might carry medical or social information MUST be omitted.
author	Classification	X	MUST NOT be used. Future versions of epSOS MAY define different protection levels for metadata and documents. Therefore all metadata elements that might carry medical or social information MUST be omitted.
confidentialityCode	Classification	R	MUST be provided for XCF compatibility but MAY be ignored by the service consumer. Value SHOULD be set to "N", as long as the Minimal Metadata Profile is not published.
formatCode	Classification	R	MUST be "urn:epSOS:ep:pre:2010" for

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013
			epSOS pivot CDA and "urn:ihe:iti:xds-sd:pdf:2008" for epSOS source coded PDF (see table 1C of [epSOS D3.5.2C]).
healthcareFacilityTypeCode	Classification	R	MUST be provided for XCF compatibility and correct addressing. Value MUST be set to ISO 3166-1 alpha-2 country code of the addressed PN.
practiceSettingCode	Classification	R	MUST be provided for XCF compatibility. Value MUST be set to "Not Used" in order to protect private patient information.
XDSDocumentEntry.uniqueId	ExternalIdentifier	R	MUST hold the OID of the document. The document unique id value MUST be the same as the value of the document's <ClinicalDocument/id> CDA header element.
XDSDocumentEntry.PatientId	ExternalIdentifier	R	MUST hold the patient identifier. The service consumer MUST verify that this id matches the patient Id that was discovered by the epSOS Identification Service.

Other metadata than the ones listed above MUST NOT be provided by the service provider. Multiple ePrescriptions (with up to two encodings) MAY be available per patient. An ebRIM association MUST be used for declaring the epSOS pivot coded document as a transformation of the source coded document. As classification scheme urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3 MUST be used per IHE-XCF. "epSOS pivot" is defined as the only code value for this epSOS valid transformation:

```
<rim:Association id="id of the association"
  associationType="urn:ihe:iti:2007:AssociationType:XFRM"
  sourceObject="UUID of the source coded document"
  targetObject="UUID of the epSOS pivot document"
```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
<rim:Classification
id="id of the classification"
classificationScheme="urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3"
classifiedObject="id of the association"
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
nodeRepresentation="epSOS pivot">
<rim:Name>
<rim:LocalizedString value="Translation into epSOS pivot format"/>
</rim:Name>
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>epSOS translation types</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:name>
<rim:LocalizedString value="Translation into epSOS pivot format" />
</rim:Name>
</rim:Classification>
</rim:Association>

```

[1] The IHE XCF profile has been accepted and is currently in Trial Implementation.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3.1.9.3 e1-REQ-4909 epSOS Order Service Errors and Warnings

Related to e1-REQ-4908 Expected Actions

If a warning is to be transmitted to the HP the ebXML Registry Error mechanism MUST be used with a syntax as defined in section 3.43.5 of IHE ITI TF 2b August 2009.

The following table lists the epSOS defined warning codes:

Warning Condition and Severity	Response Status	epSOS Warning Message (codeContext attribute)	Code (errorCode attribute)	Target
If no format qualifier is given: Not all of the requested encodings are provided (e.g. due to inability to transcode a certain national code). (ERROR)	PartialSuccess	Rendering incomplete	4101	ID of the provided ePrescription document that is missing alternative encodings
If epSOS pivot CDA format is requested: NCP-A cannot provide the minimum dataset for all its registered ePrescriptions. The HP MAY request the source coded PDF. (ERROR)	PartialSuccess	Collection incomplete	4102	None
The HP MUST consider additionally the source coded document because it MAY contain information that is not included in the epSOS pivot CDA (e.g. because field were nullified due to missing code mappings)	Success	Source coded document must be considered	2102	IDs of the affected documents

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

(WARNING)				
The prescribed medication has not been checked for interdependencies with the patient's current medication (e.g. because of country A legal restrictions). (WARNING)	Success	Dependencies not checked	2104	None
The prescription is available for dispensation but not valid for reimbursement. (WARNING)	Success	No reimbursement	2105	IDs of the affected ePrescriptions

If the epSOS Order Service provider is unable to respond with the patient's ePrescription data in the requested encoding it MUST respond with a ListResponse message that only contains a <RetrieveDocumentSetResponse/RegistryResponse> element.

For a full list of error messages defined for IHE X* see table 4.1-11 in IHE ITI TF-3 October 2008. The following table lists the additional, epSOS-specific response status types and error/warning/info codes to be used within the <RegistryErrorList> element.

Condition and Severity	Response Status	Message	Code	Action to be taken
The patient has not given consent to the requested service.	Failure	No Consent	4701	The HP SHOULD ask the patient to give consent to the requested service in country B. If the patient gives consent, the consent MUST be transmitted to country-A by using the respective operation of the epSOS consent service. If such consent giving procedure is accepted by country A, HP SHOULD re-issue the request for

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3		
		Version: 1.0		
D5.2.3		Date: 31/01/2013		

				medical data.
Country A requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation).	Failure	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechanisms (e.g. smartcard) and re-issue the request with the respective identity assertion.
Either the security policy of country A or a privacy policy of the patient (that was given in country A) does not allow the requested operation to be performed by the HP.	Failure	Insufficient Rights	4703	If the HP can switch to another (appropriate) role, he SHOULD do so and re-issue the request.
There is no ePrescription data registered for the given patient (INFO)	Success	No Data	1101	-
None of the required encodings can be provided, e.g. due to transcoding errors. (ERROR)	Failure	Transcoding Error	4203	The service provider MUST write an error log entry acc. to its respective policies.
The ePrescription registry is not accessible (ERROR)	Failure	Registry Failure	4103	
There is ePrescription data registered for the patient but the service provider is unable to access it (ERROR)	Failure	Data Access Failure	4104	The service consumer MAY re-issue the request.
The service provider is unable to evaluate the	Failure	Unknown Filter	4202	The service consumer MAY re-issue the request using another

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

given argument values (ERROR)			filter expression.
----------------------------------	--	--	--------------------

3.5.3.1.9.4 e1-REQ-4904 epSOS Order Service Security Audit Considerations

Related to e1-REQ-1838 epSOS HCP Assurance Audit Schema

Related to e1-REQ-1839 epSOS Patient Privacy Audit Schema

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in e1-REQ-1838. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in e1-REQ-1839.

The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event
Requesting Point of Care	R / X	HPO that issued the original request. This category MUST be filled by the service consumer. It MUST NOT be provided by the service provider.
Human Requestor	R	HP that triggered the request
Source Gateway	R	Service consumer node address at the country of Care
Target Gateway	R	Service provider node address at the country of the patient's affiliation
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	R	Patient
Event Target	R	Subject to the Query
Error Message	O	Only used in case that the request handling was not completed successfully

For the Event Target Category the following fields MUST be provided:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "24" (Query)
ParticipantObjectIDTypeCode	R	MUST be "10" (Search Criteria)
ParticipantObjectID	R	MUST be string-encoded UUIDs of the returned documents

3.5.3.1.9.5 e1-TXT-757 Example Request Message

The following excerpt from a epSOS Order Service list() request message shows an IHE XCF based Cross-Gateway Fetch request that contains argument slots for retrieving the available ePrescriptions (LOINC code 57833-6) of an identified patient (patient identifier 90378912821). In this example the service consumer does not specify the requested encoding. Therefore the service provider delivers both encodings (epSOS pivot and PDF/A) for all available ePrescriptions according to e1-REQ-4900.

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" ... >
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
<query:AdhocQueryRequest>
    <query:ResponseOption returnComposedObjects="true"
                           returnType="LeafClassWithRepositoryItem"/>
    <rim:AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
        <rim:Slot name="$XDSDocumentEntryPatientId">
            <rim:ValueList>
                <rim:Value>
                    '90378912821^^^&#13.6.1.4.1.21367.2005.3.7&#13;ISO'
                </rim:Value>
            </rim:ValueList>
        </rim:Slot>
        <rim:Slot name="$XDSDocumentEntryStatus">
            <rim:ValueList>
                <rim:Value>
                    ('urn:oasis:names:tc:ebxml-
regrep>StatusType:Approved')
                </rim:Value>
            </rim:ValueList>
        </rim:Slot>
    </rim:AdhocQuery>
</query:AdhocQueryRequest>

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

```

</rim:Slot>
<rim:Slot name="$XDSDocumentEntryClassCode">
  <rim:ValueList>
    <rim:Value>('57833-6^^2.16.840.1.113883.6.1')
  </rim:Value>
</rim:ValueList>
</rim:Slot>
</rim:AdhocQuery>
</query:AdhocQueryRequest>
</soapenv:Body>
</soapenv:Envelope>

```

3.5.3.1.9.6 e1-TXT-758 Example Response Messages

In this section three possible response messages to the previously sketched request message in e1-TXT-757 are shown.

The first example response message covers the case where a single ePrescription is discovered and provided as both epSOS pivot and source PDF encoding. MTOM optimization is not shown as this is a wire-format only transformation. As the epSOS Order Service list() response message is very similar to the epSOS Patient Service list() response message (see e1-TXT-756 an example) only an excerpt is shown.

```

<soapenc:Envelope>
  <soapenv:Header>....</soapenv:Header>
  <soapenv:Body>
    <query:AdhocQueryResponse
      status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">

      <rim:RegistryObjectList>

        <!-- epSOS source coded CDA wrapped PDF ePrescription document -->
        <rimext:ExtrinsicObject id="urn:uuid:cf614a65-d214-4b0d-b4b8-a0be3888f847"
          lid="urn:uuid:cf614a65-d214-4b0d-b4b8-a0be3888f847"
          objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
          status="urn:oasis:names:tc:ebxml-regrep>StatusType:Approved"
          mimeType="text/xml">

          <!-- metadata missing here (see Patient Service example) -->

          <!-- Document contents, before MTOM optimization -->
          <rimext:Document
            >UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</rimext:Document>
        </rimext:ExtrinsicObject>

        <!-- epSOS source coded CDA Pivot ePrescription document -->
        <rimext:ExtrinsicObject id="urn:uuid:eec764cf-9fe5-4101-8e86-33a13fb06e4a"
          lid="urn:uuid:eec764cf-9fe5-4101-8e86-33a13fb06e4a"
          objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

status="urn:oasis:names:tc:ebxml-regrep>StatusType:Approved"
mimeType="text/xml">

<!-- metadata missing here (see Patient Service example) -->

<!-- Document contents, before MTOM optimization -->
<rimext:Document
    >UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</rimext:Document>
</rimext:ExtrinsicObject>

<rim:Association id="urn:uuid:b4fc4809-0096-4b76-a7b1-3135ac5e5614"
    lid="urn:uuid:b4fc4809-0096-4b76-a7b1-3135ac5e5614"
    associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:XFRM"
    sourceObject="urn:uuid:eec764cf-9fe5-4101-8e86-33a13fb06e4a"
    targetObject="urn:uuid:cf614a65-d214-4b0d-b4b8-a0be3888f847"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification">
    <rim:Classification id="urn:uuid:969d2f2b-5f5a-4c24-af0a-d07d16ddae9"
        classificationScheme="urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3"
        classifiedObject="urn:uuid:b4fc4809-0096-4b76-a7b1-3135ac5e5614"
        objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
        nodeRepresentation="epSOS pivot">
        <rim:Slot name="codingScheme">
            <rim:ValueList>
                <rim:Value>epSOS translation types</rim:Value>
            </rim:ValueList>
        </rim:Slot>
        <rim:Name>
            <rim:LocalizedString value="Translation into epSOS pivot format"/>
        </rim:Name>
    </rim:Classification>
</rim:Association>

</rim:RegistryObjectList>
</query:AdhocQueryResponse>
</soapenv:Body>
</soapenv:Envelope>

```

The second example response message shows the case where two ePrescriptions are discovered. The first one is provided as epSOS pivot and source PDF encoding. For the second one country-A is not able to transform an ePrescription to the epSOS pivot format. Only the PDF encoding is provided and an information given, that epSOS pivot transcoding failed for this ePrescription. It's up to country A to decide on how to act in case of a failed epSOS pivot translation. This example covers the case where country A transmits the source coded document only. This MAY e.g. make sense in cases where both country A and B share a common language.

```

<soapenc:Envelope>
    <soapenv:Header>....</soapenv:Header>
    <soapenv:Body>
        <query:AdhocQueryResponse>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:PartialSuccess">

```

<rs:RegistryErrorList>
  <rs:RegistryError
    severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"
    errorCode="2104" codeContext="Rendering incomplete"/
    location="">
  </rs:RegistryErrorList>

  <rim:RegistryObjectList>

    <!-- ePrescription 1: epSOS source coded CDA wrapped PDF -->
    <rimext:ExtrinsicObject id="urn:uuid:cf614a65-d214-4b0d-b4b8-a0be3888f847"
      lid="urn:uuid:cf614a65-d214-4b0d-b4b8-a0be3888f847"
      objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
      status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved"
      mimeType="text/xml">

      <!-- metadata and contents missing here (see Patient Service example) -->

    </rimext:ExtrinsicObject>

    <!-- ePrescription 1: epSOS source coded CDA Pivot document -->
    <rimext:ExtrinsicObject id="urn:uuid:eec764cf-9fe5-4101-8e86-33a13fb06e4a"
      lid="urn:uuid:eec764cf-9fe5-4101-8e86-33a13fb06e4a"
      objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
      status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved"
      mimeType="text/xml">

      <!-- metadata and content missing here (see Patient Service example) -->

    </rimext:ExtrinsicObject>

    <!-- ePrescription 2: epSOS source coded CDA wrapped PDF document -->
    <rimext:ExtrinsicObject id="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-d355b57a5016"
      lid="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-d355b57a5016"
      objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
      status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved"
      mimeType="text/xml">

      <!-- metadata missing here (see Patient Service example) -->

      <!-- Document contents, before MTOM optimization -->
      <rimext:Document
        >UjBsR09EbGhjZ0dTQUxNQUFBUNBRU1tQ1p0dU1GUXhEUzhi</rimext:Document>
    </rimext:ExtrinsicObject>

    <!-- Association for ePrescription 1; for ePrescription 2 no association is
        defined because only one encoding is provided -->

    <rim:Association id="urn:uuid:b4fc4809-0096-4b76-a7b1-3135ac5e5614"
      lid="urn:uuid:b4fc4809-0096-4b76-a7b1-3135ac5e5614">

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

```

associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:XFRM"
sourceObject="urn:uuid:eec764cf-9fe5-4101-8e86-33a13fb06e4a"
targetObject="urn:uuid:cf614a65-d214-4b0d-b4b8-a0be3888f847"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification">
<rim:Classification id="urn:uuid:969d2f2b-5f5a-4c24-af0a-d07d16ddae9">
    classificationScheme="urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3"
    classifiedObject="urn:uuid:b4fc4809-0096-4b76-a7b1-3135ac5e5614"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
    nodeRepresentation="epSOS pivot">
        <rim:Slot name="codingScheme">
            <rim:ValueList>
                <rim:Value>epSOS translation types</rim:Value>
            </rim:ValueList>
        </rim:Slot>
        <rim:Name>
            <rim:LocalizedString value="Translation into epSOS pivot format"/>
        </rim:Name>
    </rim:Classification>
</rim:Association>

</rim:RegistryObjectList>
</query:AdhocQueryResponse>
</soapenv:Body>
</soapenv:Envelope>

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3.1.10 e1-FLD-178 epSOS Dispensation Service

3.5.3.1.10.1 e1-FLD-180 Initialize() Operation Request/Response Messages

3.5.3.1.10.1.1 e1-REQ-4910 Request Message

The initialize() request MUST be initiated by an HP in the country of care for handing over dispensation notifications to the patient's country of affiliation. Each dispensation notification consists of an epSOS pivot coded eDispensation document acc. to epSOS D3.5.2C and the source coded document that encodes the same information without semantic mapping. An initialize() request MAY contain multiple epSOS coded and source coded documents.

The *epSOS Dispensation Service InitializeRequest* message is a specialisation of the *IHE Provide And Register DocumentSet* transaction (ITI-41) request message as profiled in IHE XDR. The fields defined for the *ProvideAndRegisterDocumentSetRequest* message MUST be used as follows:

Element Name	epSOS Usage Convention
lcm:SubmitObjectsRequest	Container that can be used to provide the metadata for the transmitted documents, the submission set and the associations between documents (see below).
../rim:RegistryObjectList	Container that contains (pointers to) all eDispensation documents
.../rim:ExtrinsicObject	For each eDispensation document a single extrinsic object MUST be defined. There MUST be a 1:1 id-correspondence between elements and elements. For a list of further metadata to be provided with an eDispensation document see the table below.
.../rimtext:Document	base64encoded data for the eDispensation documents being submitted to the service provider. The element also includes the document id attribute (rimext:Document/@id) of type xsd:anyURI to match the document ExtrinsicObject id in the metadata and providing the necessary linkage. The base64 encoded document content MAY be encrypted. How encryption is applied and how the encryption key is negotiated should be subject to an additional specification on advanced security safeguards.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

.../rim:Association	For each pair of epSOS coded and source coded documents an ebRIM association MUST be defined (see below for details on the encoding).
---------------------	---

The service consumer SHOULD embrace the provided documents as a single IHE XDS submission set acc. to IHE ITI TF-2a August 2009. The service consumer SHOULD ignore this grouping and MUST ignore all associations between documents and submission sets. The service consumer MUST NOT process any metadata assigned to the submission set, it MUST solely rely on the document metadata and contents.

For each eDispensation document (either epSOS coded or source coded) the following set of metadata MUST be provided:

Slot Name	Binding	Slot Value
id	Attribute	Identifier of the document. This identifier MUST be the same for and .
contentType	Attribute	MUST be "text/xml"
objectType	Attribute	MUST be set acc. to section 4.3.1.2 of IHE IT TF 3 October 2008
Status	Attribute	MUST be "urn:oasis:names:tc:ebxml-regrep>StatusType:Approved"
creationTime	rim:Slot	MUST be given for XDR compatibility. SHOULD be ignored by the service provider.
languageCode	rim:Slot	MUST be given for XDR compatibility. SHOULD be ignored by the service provider.
sourcePatientID	rim:Slot	MUST be of the same value as \$XDSDocumentEntry.PatientId (see below)
healthcareFacilityTypeCode	classification	MUST be provided for XCF compatibility and correct addressing. Value MUST be set to ISO 3166-1 alpha-2 country code of the addressed PN.
practiceSettingCode	classification	MUST be provided for XDR compatibility but

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

		MAY be ignored by the service consumer. Value MUST be set to "Not Used".
confidentialityCode	classification	MUST be provided for XDR compatibility but MAY be ignored by the service consumer. Value SHOULD be set to "N", as long as the Minimal Metadata Profile is not published.
XDSDocumentClassCode	classification	eDispensation LOINC code ("60593-1")[1] coded according to specification in ITI TF-2a: 3.18.4.1.2.3.4 Coding of Code/Code-Scheme. As classification scheme 2.16.840.1.113883.6.1 MUST be used.
XDSDocumentFormatCode	classification	Format qualifier as defined in table 1C of epSOS D3.5.2C;
XDSDocumentEntry.PatientId	External identifier	Equals to the patient identifier that was provided by the epSOS Identification Service (encoded as HL7 v3 II data type)
XDSDocument.UniqueId	External identifier	MUST refer to the OID of the CDA document that is included within the element.

Other metadata than the ones listed above SHOULD NOT be provided by the service provider[2]. If given they MUST be ignored by the service consumer.
An ebRIM association MUST be used for declaring the epSOS pivot coded eDispensation document as a transformation of the source coded eDispensation document. As classification scheme urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3 MUST be used per IHE-XCF. Currently "epSOS pivot" is defined as the only valid transformation:

```

<rim:Association id="id of the association"
  associationType="urn:ihe:iti:2007:AssociationType:XFRM"
  sourceObject="UUID of the source coded document"
  targetObject="UUID of the epSOS pivot document"
  objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification">
  <rim:Classification
    id="id of the classification"
    classificationScheme="urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3"
    classifiedObject="id of the association"
    objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"

```

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

```

nodeRepresentation="epSOS pivot">
  <rim:Slot name="codingScheme">
    <rim:ValueList>
      <rim:Value>epSOS translation types</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Name>
    <rim:LocalizedString value="Translation into epSOS pivot format"/>
  </rim:Name>
  </rim:Classification>
</rim:Association>

```

[1] This code is a dummy that will be used for the initial NCP integration tests until a eDispensation LOINC code is approved.

[2] Document linkage information (e.g. a reference to the ePrescription that is affected by the dispensation) MUST be included with the document (see epSOS D2.5.2C) and MUST NOT be part of the message metadata.

3.5.3.1.10.1.2 e1-REQ-4911 Response Message (Full Success Scenario)

Related to e1-REQ-4918 Expected Actions

If the *epSOS Dispensation Service* provider is able to decode the received message and to properly process all transmitted eDispensations it responds with an *ebXML Registry Response* with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

3.5.3.1.10.1.3 e1-TXT-759 Example Request Message

The following excerpt from a *epSOS Dispensation Service InitializeRequest* message shows the transmission of a single eDispensation document:

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
  <ProvideAndRegisterDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007">
    <lcm:SubmitObjectsRequest xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0">
      <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
        <rim:ObjectRef id="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"/>
        <rim:ObjectRef id="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"/>
        <rim:ObjectRef id="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"/>
    </lcm:SubmitObjectsRequest>
  </ProvideAndRegisterDocumentSetRequest>
</soapenv:Body>
</soapenv:Envelope>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<rim:ObjectRef id="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d"/>
<rim:ObjectRef id="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"/>
<rim:ObjectRef id="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead"/>
<rim:ObjectRef id="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"/>
<rim:ObjectRef id="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"/>
<rim:ObjectRef id="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"/>
<rim:ObjectRef id="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d"/>
<rim:ObjectRef id="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983"/>
<rim:ExtrinsicObject id="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">
  <rim:Slot name="serviceStartTime">
    <rim:ValueList>
      <rim:Value>20110311</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="serviceStopTime">
    <rim:ValueList>
      <rim:Value>20110311</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="languageCode">
    <rim:ValueList>
      <rim:Value>de-AT</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="creationTime">
    <rim:ValueList>
      <rim:Value>20110311135457</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="legalAuthenticator">
    <rim:ValueList>
      <rim:Value>admin^Admin^Spirit^^^Spirit Admin
User^^^^&#216.17.710.808.1000.903.1.1.3.3&#amp;ISO</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="sourcePatientId">
    <rim:ValueList>
      <rim:Value>AT12998493069126^^^&#216.17.710.780.1000.990.1&#amp;ISO</rim:Value>
    </rim:ValueList>
  </rim:Slot>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<rim:Slot name="sourcePatientInfo">
  <rim:ValueList>
    <rim:Value>PID-
3|AT12998493069126^^^&#2.16.17.710.780.1000.990.1&#ISO</rim:Value>
    <rim:Value>PID-5|Barrel^Linda</rim:Value>
    <rim:Value>PID-7|19791105</rim:Value>
  </rim:ValueList>
</rim:Slot>
<rim:Name>
  <rim:LocalizedString value="eDispensation"/>
</rim:Name>
<rim:Description>
  <rim:LocalizedString value="eDispensation"/>
</rim:Description>
<rim:Classification classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d"
classifiedObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32952" nodeRepresentation="">
  <rim:Slot name="authorInstitution">
    <rim:ValueList>
      <rim:Value>spirit^^^^1.2.40.0.32.6.1.10&#ISO^^^^1.2.3.4.5</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="authorPerson">
    <rim:ValueList>
      <rim:Value>admin^Admin^Spirit^^Spirit Admin
User^^^^&#2.16.17.710.808.1000.903.1.1.3.3&#ISO</rim:Value>
    </rim:ValueList>
  </rim:Slot>
</rim:Classification>
<rim:Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
classifiedObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32953" nodeRepresentation="60593-1">
  <rim:Slot name="codingScheme">
    <rim:ValueList>
      <rim:Value>2.16.840.1.113883.6.1</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Name>
    <rim:LocalizedString value="eDispensation"/>
  </rim:Name>
</rim:Classification>
<rim:Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983">

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

classifiedObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
 id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32954" nodeRepresentation="60593-1">
 <rim:Slot name="codingScheme">
 <rim:ValueList>
 <rim:Value>2.16.840.1.113883.6.1</rim:Value>
 </rim:ValueList>
 </rim:Slot>
 <rim:Name>
 <rim:LocalizedString value="eDispensation"/>
 </rim:Name>
 </rim:Classification>
 <rim:Classification classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead"
 classifiedObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
 id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32955" nodeRepresentation="not used">
 <rim:Slot name="codingScheme">
 <rim:ValueList>
 <rim:Value>Connect-a-thon healthcareFacilityTypeCodes</rim:Value>
 </rim:ValueList>
 </rim:Slot>
 <rim:Name>
 <rim:LocalizedString value="not used"/>
 </rim:Name>
 </rim:Classification>
 <rim:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
 classifiedObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
 id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32956" nodeRepresentation="N">
 <rim:Slot name="codingScheme">
 <rim:ValueList>
 <rim:Value>Connect-a-thon confidentialityCodes</rim:Value>
 </rim:ValueList>
 </rim:Slot>
 <rim:Name>
 <rim:LocalizedString value="Normal"/>
 </rim:Name>
 </rim:Classification>
 <rim:Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"
 classifiedObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
 id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32957" nodeRepresentation="not used">
 <rim:Slot name="codingScheme">
 <rim:ValueList>

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<rim:Value>Connect-a-thon healthcareFacilityTypeCodes</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
  <rim:LocalizedString value="not used"/>
</rim:Name>
</rim:Classification>
<rim:Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d"
classifiedObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32958"
nodeRepresentation="urn:epSOS:ep:dis:2010">
  <rim:Slot name="codingScheme">
    <rim:ValueList>
      <rim:Value>epSOS formatCodes</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Name>
    <rim:LocalizedString value="eDispensation"/>
  </rim:Name>
  </rim:Classification>
  <rim:ExternalIdentifier id="ei:1.2.40.0.13.1.1.3052924423.20110309141024427.32959"
identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
registryObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
value="AT12998493069126^^^&#x26amp;2.16.17.710.780.1000.990.1&#x26amp;ISO">
    <rim:Name>
      <rim:LocalizedString value="XDSDocumentEntry.patientId"/>
    </rim:Name>
  </rim:ExternalIdentifier>
  <rim:ExternalIdentifier id="ei:1.2.40.0.13.1.1.3052924423.20110309141024427.32960"
identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
registryObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"
value="2.16.17.710.808.1000.902.1.1.3.2^22457B467FA5B80">
    <rim:Name>
      <rim:LocalizedString value="XDSDocumentEntry.uniqueId"/>
    </rim:Name>
  </rim:ExternalIdentifier>
  </rim:ExtrinsicObject>
  <rim:ObjectRef id="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"/>
  <rim:Association associationType="urn:ihe:iti:2007:AssociationType:XFRM"
id="as:1.2.40.0.13.1.1.3052924423.20110309141024427.32949" sourceObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fcfa6df058f4" targetObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469"/>
  <rim:ExtrinsicObject id="urn:uuid:a3c83908-1ab6-4e61-9d61-9fcfa6df058f4">

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">
  <rim:Slot name="serviceStartTime">
    <rim:ValueList>
      <rim:Value>20110311</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="serviceStopTime">
    <rim:ValueList>
      <rim:Value>20110311</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="languageCode">
    <rim:ValueList>
      <rim:Value>de-AT</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="creationTime">
    <rim:ValueList>
      <rim:Value>20110311135457</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="legalAuthenticator">
    <rim:ValueList>
      <rim:Value>admin^Admin^Spirit^^^Spirit Admin
User^^^&#216.17.710.808.1000.903.1.1.3.3&#amp;ISO</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="sourcePatientId">
    <rim:ValueList>
      <rim:Value>AT12998493069126^^^&#216.17.710.780.1000.990.1&#amp;ISO</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="sourcePatientInfo">
    <rim:ValueList>
      <rim:Value>PID-
3|AT12998493069126^^^&#216.17.710.780.1000.990.1&#amp;ISO</rim:Value>
        <rim:Value>PID-5|Barrel^Linda</rim:Value>
        <rim:Value>PID-7|19791105</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Name>
```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<rim:LocalizedString value="eDispensation"/>
</rim:Name>
<rim:Description>
<rim:LocalizedString value="eDispensation"/>
</rim:Description>
<rim:Classification classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d"
classifiedObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fca6df058f4"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32961" nodeRepresentation="">
<rim:Slot name="authorInstitution">
<rim:ValueList>
<rim:Value>spirit^^^^^1.2.40.0.32.6.1.10&ISO^^^^^1.2.3.4.5</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Slot name="authorPerson">
<rim:ValueList>
<rim:Value>admin^Admin^Spirit^^^Spirit Admin
User^^^^^&2.16.17.710.808.1000.903.1.1.3.3&ISO</rim:Value>
</rim:ValueList>
</rim:Slot>
</rim:Classification>
<rim:Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
classifiedObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fca6df058f4"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32962" nodeRepresentation="60593-1">
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>2.16.840.1.113883.6.1</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
<rim:LocalizedString value="eDispensation"/>
</rim:Name>
</rim:Classification>
<rim:Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983"
classifiedObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fca6df058f4"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32963" nodeRepresentation="60593-1">
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>2.16.840.1.113883.6.1</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
<rim:LocalizedString value="eDispensation"/>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

        </rim:Name>
        </rim:Classification>
        <rim:Classification classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead"
classifiedObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fca6df058f4"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32964" nodeRepresentation="not used">

        <rim:Slot name="codingScheme">
            <rim:ValueList>
                <rim:Value>Connect-a-thon healthcareFacilityTypeCodes</rim:Value>
            </rim:ValueList>
        </rim:Slot>
        <rim:Name>
            <rim:LocalizedString value="not used"/>
        </rim:Name>
        </rim:Classification>
        <rim:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
classifiedObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fca6df058f4"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32965" nodeRepresentation="N">
            <rim:Slot name="codingScheme">
                <rim:ValueList>
                    <rim:Value>Connect-a-thon confidentialityCodes</rim:Value>
                </rim:ValueList>
            </rim:Slot>
            <rim:Name>
                <rim:LocalizedString value="Normal"/>
            </rim:Name>
            </rim:Classification>
            <rim:Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"
classifiedObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fca6df058f4"
id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32966" nodeRepresentation="not used">

            <rim:Slot name="codingScheme">
                <rim:ValueList>
                    <rim:Value>Connect-a-thon healthcareFacilityTypeCodes</rim:Value>
                </rim:ValueList>
            </rim:Slot>
            <rim:Name>
                <rim:LocalizedString value="not used"/>
            </rim:Name>
            </rim:Classification>
            <rim:Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d"
classifiedObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fca6df058f4"

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32967" nodeRepresentation="urn:ihe:iti:xds-d:pfd:2008">
 <rim:Slot name="codingScheme">
 <rim:ValueList>
 <rim:Value>epSOS formatCodes</rim:Value>
 </rim:ValueList>
 </rim:Slot>
 <rim:Name>
 <rim:LocalizedString value="Scanned Documents PDF"/>
 </rim:Name>
 </rim:Classification>
 <rim:ExternalIdentifier id="ei:1.2.40.0.13.1.1.3052924423.20110309141024427.32968" identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427" registryObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fcfa6df058f4" value="AT12998493069126^^^×2.16.17.710.780.1000.990.1&ISO">
 <rim:Name>
 <rim:LocalizedString value="XDSDocumentEntry.patientId"/>
 </rim:Name>
 </rim:ExternalIdentifier>
 <rim:ExternalIdentifier id="ei:1.2.40.0.13.1.1.3052924423.20110309141024427.32969" identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab" registryObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fcfa6df058f4" value="2.16.17.710.808.1000.902.1.1.3.2^F942265877561AD">
 <rim:Name>
 <rim:LocalizedString value="XDSDocumentEntry.uniqueId"/>
 </rim:Name>
 </rim:ExternalIdentifier>
 </rim:ExtrinsicObject>
 <rim:ObjectRef id="urn:uuid:4b052cba-b03b-4233-8b27-e8d5e3f8d3e4"/>
 <rim:ObjectRef id="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd"/>
 <rim:ObjectRef id="urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832"/>
 <rim:ObjectRef id="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8"/>
 <rim:ObjectRef id="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446"/>
 <rim:ObjectRef id="urn:uuid:a7058bb9-b4e4-4307-ba5b-e3f0ab85e12d"/>
 <rim:ObjectRef id="urn:uuid:aa543740-bdda-424e-8c96-df4873be8500"/>
 <rim:RegistryPackage id="SubmissionSet" objectType="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd">
 <rim:Slot name="submissionTime">
 <rim:ValueList>
 <rim:Value>20110311135457</rim:Value>
 </rim:ValueList>
 </rim:Slot>

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<rim:Name>
  <rim:LocalizedString value="eDispensation"/>
</rim:Name>
<rim:Description>
  <rim:LocalizedString value="Description of eDispensation"/>
</rim:Description>
<rim:Classification classificationScheme="urn:uuid:a7058bb9-b4e4-4307-ba5b-e3f0ab85e12d"
classifiedObject="SubmissionSet" id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32970"
nodeRepresentation="">
  <rim:Slot name="authorInstitution">
    <rim:ValueList>
      <rim:Value>spirit^^^^^1.2.40.0.32.6.1.10&ISO^^^^1.2.3.4.5</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  <rim:Slot name="authorPerson">
    <rim:ValueList>
      <rim:Value>admin^Admin^Spirit^^^Spirit Admin
User^^^^^&2.16.17.710.808.1000.903.1.1.3.3&ISO</rim:Value>
    </rim:ValueList>
  </rim:Slot>
  </rim:Classification>
  <rim:Classification classificationScheme="urn:uuid:aa543740-bdda-424e-8c96-df4873be8500"
classifiedObject="SubmissionSet" id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32971"
nodeRepresentation="60593-1">
    <rim:Slot name="codingScheme">
      <rim:ValueList>
        <rim:Value>2.16.840.1.113883.6.1</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Name>
      <rim:LocalizedString value="eDispensation"/>
    </rim:Name>
    </rim:Classification>
    <rim:ExternalIdentifier id="ei:1.2.40.0.13.1.1.3052924423.20110309141024427.32972"
identificationScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8"
registryObject="SubmissionSet" value="1.2.40.0.13.1.1.3052924423.20110309141024427.32948">
      <rim:Name>
        <rim:LocalizedString value="XDSSubmissionSet.uniqueId"/>
      </rim:Name>
    </rim:ExternalIdentifier>
    <rim:ExternalIdentifier id="ei:1.2.40.0.13.1.1.3052924423.20110309141024427.32973"
identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446">

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

registryObject="SubmissionSet"
value="AT12998493069126^^^&#216.17.710.780.1000.990.1&#ISO">
<rim:Name>
  <rim:LocalizedString value="XDSSubmissionSet.patientId"/>
</rim:Name>
</rim:ExternalIdentifier>
<rim:ExternalIdentifier id="ei:1.2.40.0.13.1.1.3052924423.20110309141024427.32974">
identificationScheme="urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832"
registryObject="SubmissionSet" value="1.3.6.1.4.1.21998.1.1">
<rim:Name>
  <rim:LocalizedString value="XDSSubmissionSet.sourceId"/>
</rim:Name>
</rim:ExternalIdentifier>
</rim:RegistryPackage>
<rim:Classification classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd">
classifiedObject="SubmissionSet" id="cl:1.2.40.0.13.1.1.3052924423.20110309141024427.32975"/>
<rim:Association associationType="urn:oasis:names:tc:ebxml-
regrep:AssociationType:HasMember" id="as:1.2.40.0.13.1.1.3052924423.20110309141024427.32950">
sourceObject="SubmissionSet" targetObject="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469">
  <rim:Slot name="SubmissionSetStatus">
    <rim:ValueList>
      <rim:Value>Original</rim:Value>
    </rim:ValueList>
  </rim:Slot>
</rim:Association>
<rim:Association associationType="urn:oasis:names:tc:ebxml-
regrep:AssociationType:HasMember" id="as:1.2.40.0.13.1.1.3052924423.20110309141024427.32951">
sourceObject="SubmissionSet" targetObject="urn:uuid:a3c83908-1ab6-4e61-9d61-9fcfa6df058f4">
  <rim:Slot name="SubmissionSetStatus">
    <rim:ValueList>
      <rim:Value>Original</rim:Value>
    </rim:ValueList>
  </rim:Slot>
</rim:Association>
</rim:RegistryObjectList>
</lcm:SubmitObjectsRequest>
<Document id="urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469">
  <Include href="cid:urn:uuid:c1f32c6f-b1b7-4482-8984-9a3a9a9aa469">
  <!--#
  xmlns="http://www.w3.org/2004/08/xop/include"-->
  </Document>
<Document id="urn:uuid:a3c83908-1ab6-4e61-9d61-9fcfa6df058f4">
  <Include href="cid:urn:uuid:a3c83908-1ab6-4e61-9d61-9fcfa6df058f4">
  <!--#
  xmlns="http://www.w3.org/2004/08/xop/include"-->
  </Document>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

xmlns="http://www.w3.org/2004/08/xop/include"/>
</Document>
</ProvideAndRegisterDocumentSetRequest>
</env:Body>
</env:Envelope>

```

3.5.3.1.10.1.4 e1-TXT-760 Example Response Messages

The following example shows a possible positive response to the request given in e1-TXT-759:

```

<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <Action
      xmlns="http://www.w3.org/2005/08/addressing">urn:ihe:iti:2007:ProvideAndRegisterDocumentS
      et-bResponse</Action>
    <MessageID xmlns="http://www.w3.org/2005/08/addressing">uuid:98f4bf0c-f21a-48bc-8518-
      958c9d9dc4c11</MessageID>
    <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">uuid:98f4bf0c-f21a-48bc-8518-
      958c9d9dc4c1</RelatesTo>
  </env:Header>
  <env:Body>
    <RegistryResponse status="urn:oasis:names:tc:ebxml-
      regrep:ResponseStatusType:Success" xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"/>
  </env:Body>
</env:Envelope>

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

The following example shows a possible negative response to the request given in e1-TXT-759:

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header>...</soapenv:header>
<soapenv:Body>
  <rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
    <rs:RegistryErrorList>
      <rs:RegistryError
        severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"
        errorCode="...."
        codeContext="No Match"
        location="" />
    </rs:RegistryErrorList>
  </rs:RegistryResponse>
</soapenv:Body>
</soapenv:Envelope>

```

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3.1.10.2 e1-FLD-182 Discard() Operation Request/Response Messages

3.5.3.1.10.2.1 e1-REQ-4919 Request Message

The *epSOS Dispensation Service* discard() request is initiated by an HP in the country of care (country B) for deleting a previously transmitted eDispensation document at the patient's country of affiliation (country A). The respective request message corresponds to the ebXML 3.0 RemoveObjectsRequest message. The fields defined for the ebXML 3.0 RemoveObjectsRequest MUST be used as defined in IHE XDS Metadata Update:

Element Name	epSOS Usage Convention
ObjectRefList	List of all eDispensation objects that have been erroneously sent to country A
ObjectRef	For each eDispensation object, submission set and association to discard. There MUST be a single ObjectRef element
@id	The id-attribute MUST refer to the object identifier as given in the metadata of the object to be deleted.

In order to completely discard a previously transmitted eDispensation package, all of the following objects MUST be referenced in the <ObjectRefList>:

epSOS coded eDispensations

PDF/A source coded eDispensations

Associations between epSOS coded and source coded documents

Submission set (for discarding the submission set metadata)

Associations between documents and the submission set

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.5.3.1.10.2.2 e1-REQ-4920 Response Message (Full Success Scenario)

Related to e1-REQ-4927 Expected Actions

If the *epSOS Dispensation Service* provider is able to decode the received dispensation document IDs and to properly process the request, it responds with an *ebXML Registry Response* with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

```
<rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
</rs:RegistryResponse>
```

3.5.3.1.10.2.3 e1-TXT-761 Example Request Message

The following excerpt from a *epSOS Dispensation Service* `discard()` request message shows the deletion of a single eDispensation document (the one that was transmitted in the example in e1-TXT-759).

```
<soapenv:Envelope xmlns...>
  <soapenv:Header>
    ...
  </soapenv:Header>
  <soapenv:Body>
    <lcm:RemoveObjectsRequest
      xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
      xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
      <ObjectRefList xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">

        <!-- epSOS pivot CDA eDispensation document -->
        <ObjectRef id="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"/>

        <!-- epSOS source coded CDA wrapped PDF eDispensation document -->
        <ObjectRef id="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-d355b57a5016"/>

        <!-- These IDs are not shown in the eDispensation example
            (submitted with symbolic names instead of UUIDs)
            so these are ids are made up for this example -->

        <!-- XFRM association -->
```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<ObjectRef id="urn:uuid:822441f0-1644-42bf-9dce-
f718598beb13"/>

    <!-- SubmissionSet -->
    <ObjectRef id="urn:uuid:cafddedeb-d13c-4242-b27b-
cf2bf9644748"/>

        <!-- SubmissionSet to pivot CDA eDispensation
documentAssociation -->
        <ObjectRef id="urn:uuid:41b4d56b-2e8b-4490-b804-
ea60ec5f8a67"/>

            <!-- SubmissionSet to source coded CDA wrapped PDF
eDispensation Assoc. -->
            <ObjectRef id="urn:uuid:b9e91e88-7186-48df-bc51-
c2e2a0db78d5"/>
        </ObjectRefList>
    </lcm:RemoveObjectsRequest>
</soapenv:Body>
</soapenv:Envelope>

```

3.5.3.1.10.2.4 e1-TXT-762 Example Response Messages

The following example shows a possible positive response to the request given in e1-TXT-761:

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header>...</soapenv:Header>
<soapenv:Body>
<rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
</rs:RegistryResponse>
</soapenv:Body>
</soapenv:Envelope>

```

The following example shows a possible negative response to the request given in e1-TXT-761:

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header>...</soapenv:Header>
<soapenv:Body>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

```

<rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
<rs:RegistryErrorList>
<rs:RegistryError
    severity="urn:oasis:names:tc:ebxml-regrep>ErrorSeverityType:Error"
    errorCode="...."
    codeContext="No Match"
    location="1.42.20100103225206.3.3" />
</rs:RegistryErrorList>
</rs:RegistryResponse>
</soapenv:Body>
</soapenv:Envelope>

```

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

3.5.3.1.10.3 e1-FLD-183 epSOS Dispensation Service Errors and Warnings

3.5.3.1.10.3.1 e1-REQ-4924 Initialize() Operation Errors and Warnings

Related to e1-REQ-4918 Expected Actions

If the service provider wants to respond with further information on the processing of the transmitted data or with a non-critical warning it SHOULD include an additional <RegistryErrorList> element. The severity MUST be set to “urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning”:

```
<rs:RegistryResponse
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
<rs:RegistryErrorList>
    <rs:RegistryError
        severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning"
        errorCode="...."
        codeContext="Processing deferred"
        location="" />
</rs:RegistryErrorList>
</rs:RegistryResponse>
```

The following warning messages and codes are defined:

Condition and Severity	Message	Code	Action to be taken
eDisensations were received but not processed	Processing deferred	2201	None

If the *epSOS Dispensation Service* provider is able to decode the received message but the processing of one or more dispensations failed, it responds with an *ebXML Registry Response* that contains a respective status indicator (see below). The response MUST contain a RegistryErrorList element that indicates the failure condition.

If none of the eDisensations was processed successfully, the response status MUST be set to “urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”. If at least one eDispensation was processed successfully, the response status MUST be set to “urn:ihe:iti:2007:ResponseStatusType:PartialSuccess”.

A failure location MUST be provided if the error does not apply to all provided eDispensation documents. It MUST NOT be given if the error applies to all provided documents.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The severity of each registry error message MUST be set to "urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error". Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of IHE ITI TF-3 October 2008 the following error codes are defined for epSOS:

Condition and Severity	Location	Message	Code	Action to be taken
No matching ePrescription was found (ERROR)	OID of the eDispensation document that caused the error.	No match	4105	HP-B (or NCP-B depending on the concrete implementation) SHOULD check the document IDs and re-issue the request.
ePrescription has already been dispensed (ERROR)	OID of the eDispensation document that caused the error.	Invalid Dispensation	4106	HP-B SHOULD again query for the list of available ePrescription.
Country A requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	-	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechanisms (e.g. smartcard) and re-issue the request with the respective identity assertion.
The eDispensation service provider only accepts dispensation data that is digitally signed by an HP. (ERROR)	OID of the eDispensation document that caused the error.	No Signature	4704	If possible, NCP-B SHOULD re-issue the request with the data signed by an HP.
The service consumer did not provide the source coded PDF document for an eDispensation (ERROR)	OID of the epSOS coded eDispensation that is not additionally	Original data missing	4107	The epSOS pivot coded document MUST NOT be processed by the service provider. The service consumer

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

	provided as source coded document			MUST re-transmit the dispensation with both encodings.
The service consumer did not provide the epSOS pivot coded document for an eDispensation (ERROR)	OID of the source coded eDispensation that is not additionally provided as epSOS pivot coded document	Pivot data missing	4108	The source coded document MUST NOT be processed by the service provider. The service consumer MUST re-transmit the dispensation with both encodings.

3.5.3.1.10.3.2 e1-REQ-4922 Discard() Operation Errors and Warnings

Related to e1-REQ-4927 Expected Actions

If the *epSOS Dispensation Service* provider is able to decode the received dispensation document IDs but the deprecating of the dispensations failed, it responds with an *ebXML Registry Response* that contains a respective status indicator (see below). The response MUST contain a *RegistryErrorList* element that indicates the failure condition.

If none of the eDispensations was deprecated successfully, the response status MUST be set to “urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”. If at least one eDispensation was deprecated successfully, the response status MUST be set to “urn:ihe:iti:2007:ResponseStatusType:PartialSuccess”.

A failure location MUST be provided if the error does not apply to all to-be-deprecated eDispensation documents. It MUST NOT be given if the error applies to all documents that are to be deprecated.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The severity of each registry error message MUST be set to "urn:oasis:names:tc:ebxml-regrep>ErrorSeverityType:Error". Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. In extension to the XDS-b error messages defined in Table 4.1-11 of IHE ITI TF-3 October 2008 the following error codes are defined for epSOS:

Condition	Location	Message	Code	Action to be taken
No matching eDispensation was found	OID of the document that could not be found	No match	4105	The HP SHOULD check the OID of the document and re-issue the request
Request is rejected because the issuing HCPO of the discard request is not the HCPO that provided the eDispensation.	OID of the document that caused the error	Insufficient rights	4703	Patient SHOULD ensure that the discard request is issued by the same HCPO that did the dispensation. If the ePrescription was dispensed at another HCPO the patient MUST request for discarding at this HCPO.
Request was accepted but will not be processed immediately	-	Processing deferred	2201	No action needed. HP and patient MUST be aware that the respective prescription cannot be dispensed again immediately.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3.1.10.4 e1-FLD-184 epSOS Dispensation Service Security Audit Considerations

3.5.3.1.10.4.1 e1-REQ-4925 Initialize() Operation Security and Audit Considerations

Related to e1-REQ-1838 epSOS HCP Assurance Audit Schema

Related to e1-REQ-1839 epSOS Patient Privacy Audit Schema

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in e1-REQ-1838. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in e1-REQ-1839.

The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epSOS Instance	Opt.	Description
Event	R	Audited event
Requesting Point of Care	R / X	HCPO that issued the original request. This category MUST be filled by the service consumer. It MUST NOT be provided by the service provider.
Human Requestor	R	HCP that triggered the request
Source Gateway	R	Service consumer node address at the country of Care
Target Gateway	R	Service provider node address at the country of the patient's affiliation
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	R	Patient
Event Target	R	References to the provided dispensation documents (see below)
Error Message	O	Only used in case that the request handling was not completed successfully

For the Event Target Category the following fields MUST be provided:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "4" (Resource)
ParticipantObjectIDTypeCode	R	MUST be "12" (URI)
ParticipantObjectID	R	MUST be string-encoded UUIDs of the provided documents

3.5.3.1.10.4.2 e1-REQ-4923 Discard() Operation Security and Audit Considerations

Related to e1-REQ-1838 epSOS HCP Assurance Audit Schema

Related to e1-REQ-1839 epSOS Patient Privacy Audit Schema

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in e1-REQ-1838. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in e1-REQ-1839.

 epsOS <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

epsOS Instance	Opt.	Description
Event	R	Audited event
Requesting Point of Care	R / X	HCPO that issued the original request. This category MUST be filled by the service consumer. It MUST NOT be provided by the service provider.
Human Requestor	R	HCP that triggered the request
Source Gateway	R	Service consumer node address at the country of Care
Target Gateway	R	Service provider node address at the country of the patient's affiliation
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Patient	R	Patient
Event Target	R	Reference to the discarded document
Error Message	O	Only used in case that the request handling was not completed successfully

For the Event Target Category the following fields MUST be provided:

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "4" (Resource)
ParticipantObjectDataLifeCycle	R	MUST be "14" (logical deletion)
ParticipantObjectIDTypeCode	R	MUST be "12" (URI)
ParticipantObjectID	R	MUST be string-encoded UUIDs of the discarded documents

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3.2 e1-FLD-173 Computational Dimension

3.5.3.2.1 e1-FLD-177 epSOS Order Service

3.5.3.2.1.1 e1-REQ-4903 epSOS Order Service Message Specification

Related to e1-REQ-4842 epSOS OrderService Service Interface & Functional Specification

Related to e1-REQ-4883 epSOS Trusted Service List

The epSOS Order Service MUST be used to share an identified patient's ePrescriptions between the patient's country of affiliation and the country of care. Both countries are represented by their respective NCPs.

The implementation of the *epSOS Order Service* is based on the following standards:

ebRIM: OASIS/ebXML Registry Information Model v3.0 OASIS ebRIM 3.0

ebRS: OASIS/ebXML Registry Services Specifications v3.0[1] OASIS ebRS 3.0

MTOM: SOAP Message Transmission Optimization Mechanism W3C MTOM

XOP: XML-binary Optimized Packaging W3C XOP

and:

XCF: IHE Cross-Community Fetch IHE XCF

For discovery and localisation of the Order Service instance that is responsible for providing access to the identified patient's data see e1-REQ-4883.

[1] The integration of ebRS and MTOM as used by epSOS is not compatible with the current version of OASIS ebRS.

3.5.3.2.1.1.1 e1-REQ-4907 List() Operation

The *epSOS Order Service* list() operation is implemented as an IHE XCF Cross-Gateway Fetch transaction. It is fully compliant with the ebRS 3.0 standard. The *epSOS Order Service* list() operation includes the documents listed in the response meta-data, just like they would have been included in Cross-Gateway Retrieve (SOAP 1.2 MTOM with XOP encoding attachments).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3.2.1.1.1.1 e1-REQ-4908 Expected Actions

Related to e1-REQ-4557 NFR01- Service availability

Related to e1-REQ-4566 NFR10- Guaranteed delivery

Related to e1-REQ-4909 epSOS Order Service Errors and Warnings

Related to e1-REQ-4860 Exception Handling

Related to e1-REQ-4901 Response Message (Full Success Scenario)

The epSOS Order Service provider shall respond to a ListRequest message with the ListResponse message containing

the identified patient's available ePrescriptions together with a status notification (full success scenario) or

an error message (epSOS Order Service Error and Warnings).

The epSOS Order Service provider MUST verify that the requesting service user has sufficient rights to access the available ePrescriptions of the identified patient.

In case of an error that relates to the transmission of the request or the processing of the epSOS security token, the epSOS Order Service provider MUST respond with a fault message according to e1-REQ-4860.

3.5.3.2.1.2 e1-REQ-4905 epSOS Order Service Protocol Requirements

Related to e1-REQ-1883 epSOS Common Message Format

The epSOS Order Service List() request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in e1-REQ-1883.

Port types and bindings MUST be used as defined in the WSDL given in e1-REQ-4906. Acc. to this the epSOS Order Service List() operation's request and response data MUST be contained within the message body as follows:

epSOS Patient Service	Message Body
List request	CrossGatewayQueryRetrieve_Message (see e1-REQ-4906)
List response	CrossGatewayQueryRetrieveResponse_Message (see e1-REQ-4906)

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

The request message MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in e1-REQ-4884. The response message MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in e1-REQ-4884.

3.5.3.2.1.2.1 e1-REQ-4906 IHE XCA Responding Gateway Query-Retrieve WSDL

```

<?xml version="1.0" encoding="UTF-8"?>
<definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:ihe="urn:ihe:iti:xds-b:2007" xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
  xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
  xmlns:xdsext="urn:ihe:iti:xds-ebrim:extensions:2010"
  targetNamespace="urn:ihe:iti:xds-b:2007"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
  name="RespondingGateway_QueryRetrieve">
  <documentation>IHE XCA Responding Gateway Query Retrieve</documentation>
  <types>
    <xsd:schema elementFormDefault="qualified">
      <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
        schemaLocation="../schemas/rs.xsd"/>
      <xsd:import namespace="urn:ihe:iti:xds-b:2007"
        schemaLocation="../schemas/XDS.b_DocumentRepository.xsd"/>
      <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
        schemaLocation="../schemas/query.xsd"/>
    </xsd:schema>
  </types>
  <message name="CrossGatewayQueryRetrieve_Message">
    <documentation>Cross Gateway Query Retrieve</documentation>
    <part name="body" element="query:AdhocQueryRequest"/>
  </message>
  <message name="CrossGatewayQueryRetrieveResponse_Message">
    <documentation>Cross Gateway Query RetrieveResponse</documentation>
    <part name="body" element="query:AdhocQueryResponse"/>
  </message>
  <portType name="RespondingGatewayQueryRetrieve_PortType">
    <operation name="RespondingGateway_CrossGatewayQueryRetrieve">
      <input message="ihe:CrossGatewayQueryRetrieve_Message"
        wsaw:Action="urn:ihe:iti:2010:CrossGatewayQueryRetrieve"/>
      <output message="ihe:CrossGatewayQueryRetrieveResponse_Message"
        wsaw:Action="urn:ihe:iti:2010:CrossGatewayQueryRetrieveResponse"/>
    </operation>
  </portType>
</definitions>

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

        </operation>
    </portType>
<binding name="RespondingGatewayQueryRetrieve_Binding_Soap12"
    type="ihe:RespondingGatewayQueryRetrieve_PortType">
    <soap12:binding style="document"
        transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="RespondingGateway_CrossGatewayQueryRetrieve">
        <soap12:operation
            soapAction="urn:ihe:iti:2010:CrossGatewayQueryRetrieve"/>
        <input>
            <soap12:body use="literal"/>
        </input>
        <output>
            <soap12:body use="literal"/>
        </output>
    </operation>
</binding>
<service name="RespondingGatewayQueryRetrieve_Service">
    <port name="RespondingGatewayQueryRetrieve_Port_Soap12"
        binding="ihe:RespondingGatewayQueryRetrieve_Binding_Soap12">
        <soap12:address
            location="http://servicelocation/RespondingGatewayQueryRetrieve_Service"/>
    </port>
</service>
</definitions>
```

3.5.3.2.2 e1-FLD-179 epSOS Dispensation Service

3.5.3.2.2.1 e1-REQ-4914 epSOS Dispensation Service Message Specification

Related to e1-REQ-4843 epSOS DispensationService Service Interface & Functional Specification

Related to e1-REQ-4883 epSOS Trusted Service List

The *epSOS Dispensation Service* MUST be used to share an identified patient's eDispensation data between the patient's country of affiliation and the country of care. Both countries are represented by their respective NCPs.

The implementation of the *epSOS Dispensation Service* is based on the following standards:

ebRIM: OASIS/ebXML Registry Information Model v3.0 OASIS ebRIM 3.0

ebRS: OASIS/ebXML Registry Services Specifications v3.0[1] OASIS ebRS 3.0

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

MTOM: SOAP Message Transmission Optimization Mechanism W3C MTOM

XOP: XML-binary Optimized Packaging W3C XOP

and is compliant with the IHE profiles:

XDR: IHE Cross-Enterprise Reliable Exchange IHE XDR

For discovery and localisation of the *epSOS Dispensation Service* instance that is responsible for providing access to the identified patient's data see e1-REQ-4883.

3.5.3.2.2.1.1 e1-REQ-4917 Initialize() Operation

The *epSOS Dispensation Service* initialize() operation is implemented by the *IHE Provide And Register DocumentSet* transaction (ITI-41) as described in IHE XDR.

3.5.3.2.2.1.1.1 e1-REQ-4918 Expected Actions

Related to e1-REQ-4557 NFR01- Service availability

Related to e1-REQ-4566 NFR10- Guaranteed delivery

Related to e1-REQ-4860 Exception Handling

Related to e1-REQ-4924 Initialize() Operation Errors and Warnings

Related to e1-REQ-4911 Response Message (Full Success Scenario)

The *epSOS Dispensation Service* provider shall respond to an InitializeRequest message with the InitializeResponse message containing a success indicator.

The *epSOS Dispensation Service* provider MUST verify that the requesting service user has sufficient rights to submit an eDispensation for the identified patient. It MUST verify that the eDispensation matches with an ePrescription that was issued for the identified patient.

In case of an error that relates to the transmission of the request or the processing of the epSOS security token, the *epSOS Dispensation Service* provider MUST respond with a fault message according to e1-REQ-4860.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.5.3.2.2.1.2 e1-REQ-4921 Discard() Operation

The *epSOS Dispensation Service* discard() operation SHOULD be used to deprecate a previously transmitted eDispensation. It is implemented by the ebXML RemoveObjectsRequest registry operation as profiled in the IHE Draft Profile on XDS Metadata Update.

3.5.3.2.2.1.2.1 e1-REQ-4927 Expected Actions

Related to e1-REQ-4922 Discard() Operation Errors and Warnings

Related to e1-REQ-4860 Exception Handling

Related to e1-REQ-4920 Response Message (Full Success Scenario)

The *epSOS Dispensation Service* provider shall remove all registry objects and documents as identified in the request. It shall respond to a DiscardRequest message with a registry response message containing a success indicator.

The *epSOS Dispensation Service* service provider MUST verify that the requesting service user has sufficient rights to delete an eDispensation for the identified patient. It MUST verify that the eDispensation was issued by the same HPO that now wants to discard it.

In case of an error that relates to the transmission of the request or the processing of the epSOS security token, the *epSOS Dispensation Service* provider MUST respond with a fault message according to e1-REQ-4860.

3.5.3.2.2.2 e1-REQ-4915 epSOS Dispensation Service Protocol Requirements

Related to e1-REQ-1883 epSOS Common Message Format

The *epSOS Dispensation Service* operations' request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in e1-REQ-1883.

Port types and bindings MUST be used as defined in the WSDLs given in e1-REQ-4916 (initialize operation) and e1-REQ-4926 (discard operation). Acc. to this the *epSOS Dispensation Service* operations' request and response data MUST be contained within the message body as follows:

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

epSOS Dispensation Service	Message Body
Initialize request	ProvideAndRegisterDocumentSet-b_Message (see e1-REQ-4916)
Initialize response	ProvideAndRegisterDocumentSet-bResponse_Message (see e1-REQ-4916)
Discard request	DeleteMetadata_Message (see e1-REQ-4926)
Discard response	DeleteMetadataResponse_Message (see section e1-REQ-4926)

epSOS Dispensation Service request messages MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in e1-REQ-4884. *epSOS DispensationService* response messages MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in e1-REQ-4884.

3.5.3.2.2.1 e1-REQ-4916 IHE XDR Document Recipient WSDL

```

<?xml version="1.0" encoding="utf-8"?>
<definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:ihe="urn:ihe:iti:xds-b:2007"
  xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
  targetNamespace="urn:ihe:iti:xds-b:2007"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" name="DocumentRecipient">
  <documentation>IHE Document Recipient</documentation>
  <types>
    <xsd:schema elementFormDefault="qualified"
      targetNamespace="urn:ihe:iti:xds-b:2007"
      xmlns:ihe="urn:ihe:iti:xds-b:2007">
      <!-- Include the message schema -->
      <xsd:include schemaLocation="../schemas/IHE/XDS.b_DocumentRecipient.xsd"/>
    </xsd:schema>
    <xsd:schema elementFormDefault="qualified"
      targetNamespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0">
<!-- Include the message schema -->
<xsd:include schemaLocation="../schemas/ebRS/rs.xsd"/>
</xsd:schema>
<!-- While no elements are directly used from these schema in the WSDL,
they need to be present here in order for
code generating toolkits to work properly -->
<xsd:schema elementFormDefault="qualified"
targetNamespace="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0">
<!-- Include the message schema -->
<xsd:include schemaLocation="../schemas/ebRS/lcm.xsd"/>
</xsd:schema>
<xsd:schema elementFormDefault="qualified"
targetNamespace="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
<!-- Include the message schema -->
<xsd:include schemaLocation="../schemas/ebRS/rim.xsd"/>
</xsd:schema>
</types>
<message name="ProvideAndRegisterDocumentSet-b_Message">
<documentation>Provide and Register Document Set</documentation>
<part name="body" element="ihe:ProvideAndRegisterDocumentSetRequest"/>
</message>
<message name="ProvideAndRegisterDocumentSet-bResponse_Message">
<documentation>Provide And Register Document Set Response</documentation>
<part name="body" element="rs:RegistryResponse"/>
</message>
<binding name="DocumentRecipient_Binding" type="ihe:DocumentRecipient_PortType">
<soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
<operation name="DocumentRecipient_ProvideAndRegisterDocumentSet-b">
<soap12:operation soapAction="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"/>
<input>
<soap12:body use="literal"/>
</input>
<output>
<soap12:body use="literal"/>
</output>
</operation>
</binding>
<service name="DocumentRecipient_Service">
<port name="DocumentRecipient_Port_Soap12" binding="ihe:DocumentRecipient_Binding">

```

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

```

<soap12:address location="http://servicelocation/DocumentRecipient_Service"/>
</port>
</service>
</definitions>

```

3.5.3.2.2.2 e1-REQ-4926 IHE XDR Metadata Update Delete WSDL

```

<?xml version="1.0" encoding="UTF-8"?>
<definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:ihe="urn:ihe:iti:xds-b:2007"
  xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
  xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
  xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
  xmlns:xdsext="urn:ihe:iti:xds-ebrim:extensions:2010"
  targetNamespace="urn:ihe:iti:xds-b:2007"
  xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
  name="RespondingGateway_QueryRetrieve">
  <documentation>OASIS ebXML Registry Remove Objects operation</documentation>
  <types>
    <xsd:schema elementFormDefault="qualified">
      <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
        schemaLocation="../schemas/rs.xsd"/>
      <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
        schemaLocation="../schemas/lcm.xsd"/>
      <xsd:import namespace="urn:ihe:iti:xds-b:2007"
        schemaLocation="../schemas/XDS.b_DocumentRepository.xsd"/>
      <xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
        schemaLocation="../schemas/query.xsd"/>
    </xsd:schema>
  </types>
  <message name="DeleteMetadata_Message">
    <documentation>Delete Metadata</documentation>
    <part name="body" element="lcm:RemoveObjectsRequest"/>
  </message>
  <message name="DeleteMetadataResponse_Message">
    <documentation>Delete Metadata Response</documentation>
    <part name="body" element="rs:RegistryResponse"/>
  </message>
  <portType name="DocumentRecipientDeleteMetadata_PortType">
    <operation name="DocumentRecipient_DeleteMetadata">

```

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

```

<input message="lcm:RemoveObjectsRequest"
       wsaw:Action="urn:ihe:iti:2010:DeleteDocumentSet"/>
<output message="rs:RegistryResponse"
       wsaw:Action="urn:ihe:iti:2010:DeleteDocumentSetResponse"/>
</operation>
</portType>
<binding name="DocumentRecipientDeleteMetadata_Binding_Soap12"
         type="ihe:DocumentRecipientDeleteMetadata_PortType">
<soap12:binding style="document"
                 transport="http://schemas.xmlsoap.org/soap/http"/>
<operation name="DocumentRecipient_DeleteMetadata">
<soap12:operation soapAction="urn:ihe:iti:2010:DeleteDocumentSet"/>
<input>
<soap12:body use="literal"/>
</input>
<output>
<soap12:body use="literal"/>
</output>
</operation>
</binding>
<service name="DocumentRecipientDeleteMetadata_Service">
<port name="DocumentRecipientDeleteMetadata_Port_Soap12"
      binding="ihe:DocumentRecipientDeleteMetadata_Binding_Soap12">
<soap12:address
location="http://servicelocation/DocumentRecipientDeleteMetadata_Service"/>
</port>
</service>
</definitions>

```

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6 e1-FLD-64 Healthcare Encounter Report (HCER) Service Specification

3.6.1 e1-FLD-82 Conceptual Perspective

3.6.1.1 e1-FLD-247 Information Dimension

3.6.1.1.1 e1-REQ-5138 About Patient Identification in the ePrescription

Synchronized with e1-REQ-1668 About Patient Identification in the ePrescription

Variable	Definitions	MS: Minimum Optional	Comments	Example
Given Name	The Name of the patient	Yes	This field can contain more than one element	Marta
Family Name/Surname	The surname/s of the patient	Yes	This field can contain more than one element	Español Smith
Gender	The gender of the patient	Yes		Male/female/unknown
Birth date	Date of birth	Yes	This field may contain only the year	01/01/2009
Regional/National Health Id	If the patient has a regional or national Health Identification	Yes	This field is required by some national laws	
Social/Insurance Number		Yes	If a patient has both, national/regional ID and Social/Insurance number, only the regional/national Health Id is required by law. If the only identification the patient has is the Social/insurance number, then this one is considered as the regional/national Health Id. This	

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

		field is required by some national laws.	
--	--	--	--

3.6.1.1.2 e1-REQ-5144 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-1669 About HP Prescriber Identification in the ePrescription

Variable	Definitions	MS: Minimum Max: maximum	Comments	Example
Given Name	The Name of the Prescriber	MS	This field can contain more than one element	Marta
Family name/surname	The surname/s of the Prescriber	MS	This field can contain more than one element	Español Smith
HP Id number	The identification of the person as HP	MS		12345
Profession		MS		Physician
Specialist		Max		Dermatologist
Prescriber Facility Address:	The place (complete address) where the prescriber made the prescription		This is not a field but a block of information made up of the following fields. This might not be in the dataset but this information needs to be available for the process traceability (FR20)	e.g., Los Bermejales Health Care Centre. Alemania St. Seville, 41018. Spain
Name of the		Max		For instance, the name of the

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

Facility				building: Los Berrmejales
Street Address		Max		Alemania Street
City		Max		Seville
State or Province		Max		Seville
Zip or Postal Code		Max		41018
Telephone		Max		+34 954123123
Contact email of the centre or of the prescriber		Max		losbermejaleshealthcentre@xxx.es
Country	The country where the prescription was made	MS	The dispenser needs to know the country where he is consulting the information from	Spain
Prescriber Organization:			This is not a field but a block of information made up of the following fields. This might not be in the dataset but this information needs to be available for the process traceability (FR20)	
Organization Name		Max		e.g. Andalusia Health Service
Organization Identifier		Max	This field can be numbers and/or letters	123458xfs

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.1.2 e1-FLD-134 Computational Dimension

3.6.1.2.1 e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Related to e1-REQ-5092 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-5105 Data Integrity

Related to e1-REQ-5119 Data Origin and Data Authenticity

Related to e1-REQ-2099 FR01 Utilization of NCP-B Portal for HCER documentation by Health professional in country B

Related to e1-REQ-2100 HCER-FR02 Country A is informed of treatment event in country B

Related to e1-REQ-2106 HCER-FR06 Information Traceability

Related to e1-REQ-2124 HCER-FR14 Forwarding HCER

Related to e1-REQ-2120 HCER-NFR01 Service Availability

Related to e1-REQ-2121 HCER-NFR02 Response time

Related to e1-REQ-2123 HCER-NFR03 New document type

Related to e1-REQ-4991 HP-B Identification and Authentication

Related to e1-REQ-5097 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-5124 Minimum and Maximum Data Sets

Related to e1-REQ-5123 NFR05- Access control

Related to e1-REQ-5095 NFR09- Trust between countries

Related to e1-REQ-5115 NFR10- Guaranteed delivery

Related to e1-REQ-5117 NFR12- Supervision services

Related to e1-REQ-5077 Patient Identification

Related to e1-REQ-5126 Peering Original Document

Related to e1-REQ-5127 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-5099 Structured Information and Semantic Compliance

Related to e1-REQ-5081 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-4571 UC.PS.6 Patient Summary Extension

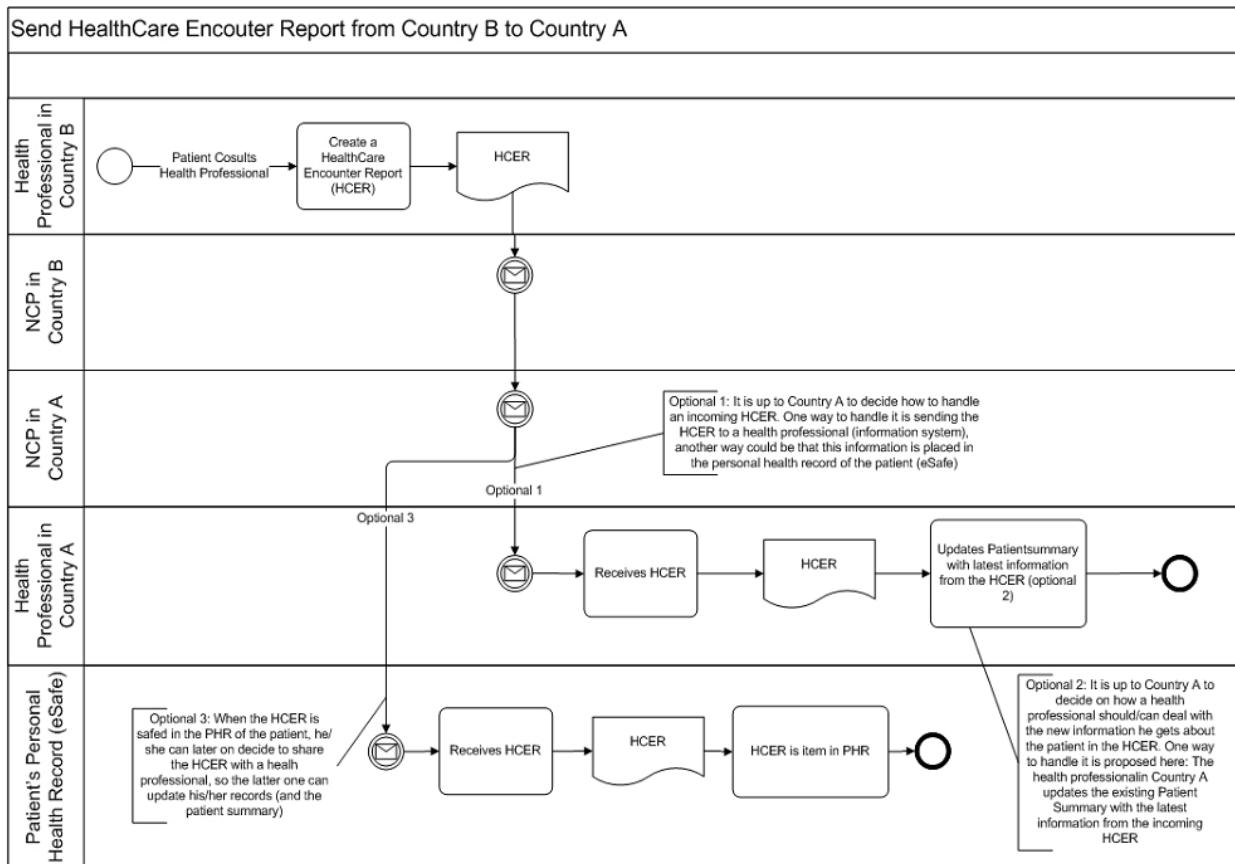
Related to e1-REQ-5085 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-5089 Willful Provisioning of Data (»Consent-1«)

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Related to e1-TXT-664 Service Pre-requisites

The HCER supports the patient summary extension use case UC.PS.6 as described in D.1.4.1. In this use case, after a PS is retrieved by country B, country A is informed on the healthcare encounter in country B, so country A is able to update the history of the patient summary (according to its own policies).



Note that the health professional in country B has to be identified and authenticated and he/she has to validate the identity of the patient and the existence of his/her consent. These steps are not depicted in the diagram above. Also: after the NCP in country A has received the HCER, it is the responsibility of country A to take further action. Country A is entitled to take no further action. This is a decision to be taken by country A and is out of scope of the epSOS phase 2 specifications.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.6.1.2.2 e1-TXT-664 Service Pre-requisites

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Related to e1-REQ-3844 MRO Service State Diagram

The service precondition consists of the following elements:

Country A is responsible for keeping the medical information of its own patients up-to-date. These specifications do not make any assumptions on how medical data is managed within a country A.

Country A must provide, maintain and support the NCP supporting communication of the information identified in this section with country B and vice versa and that there must be a chain of trust between system actors in this process. Transaction logging and transport security are available in both country A and B.

Services for identification and authentication of health professionals are available in country B, in a way country B can provide country A with sufficient information to authorize the data access of the health professional of country B.

Patient identification service is available: Country A shall offer the health professional in country B means to validate the identity of the patient.

Legal compliance: Original medical document ownership (owner is both the patient and the entity where the document is stored) and medical / legal validity of transformed document shall be analysed according to the different PN's laws.

Semantic interoperability of structured clinical content: information sent is understandable (in the correct context) for the receiver.

Scalability: The implementation should scale well with respect to the number of documents exchanged

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.1.2.3 e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-5092 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-5105 Data Integrity

Related to e1-REQ-5119 Data Origin and Data Authenticity

Related to e1-REQ-2099 FR01 Utilization of NCP-B Portal for HCER documentation by Health professional in country B

Related to e1-REQ-2100 HCER-FR02 Country A is informed of treatment event in country B

Related to e1-REQ-2106 HCER-FR06 Information Traceability

Related to e1-REQ-2111 HCER-FR09 Link HCERs

Related to e1-REQ-2124 HCER-FR14 Forwarding HCER

Related to e1-REQ-2120 HCER-NFR01 Service Availability

Related to e1-REQ-2121 HCER-NFR02 Response time

Related to e1-REQ-2123 HCER-NFR03 New document type

Related to e1-REQ-4991 HP-B Identification and Authentication

Related to e1-REQ-5097 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-5124 Minimum and Maximum Data Sets

Related to e1-REQ-5123 NFR05- Access control

Related to e1-REQ-5095 NFR09- Trust between countries

Related to e1-REQ-5115 NFR10- Guaranteed delivery

Related to e1-REQ-5117 NFR12- Supervision services

Related to e1-REQ-5077 Patient Identification

Related to e1-REQ-5126 Peering Original Document

Related to e1-REQ-5127 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-5099 Structured Information and Semantic Compliance

Related to e1-REQ-5081 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-4575 UC.MED.2 Medicine newly prescribed in country B

Related to e1-REQ-5085 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-5089 Willful Provisioning of Data (»Consent-1«)

Related to e1-TXT-664 Service Pre-requisites

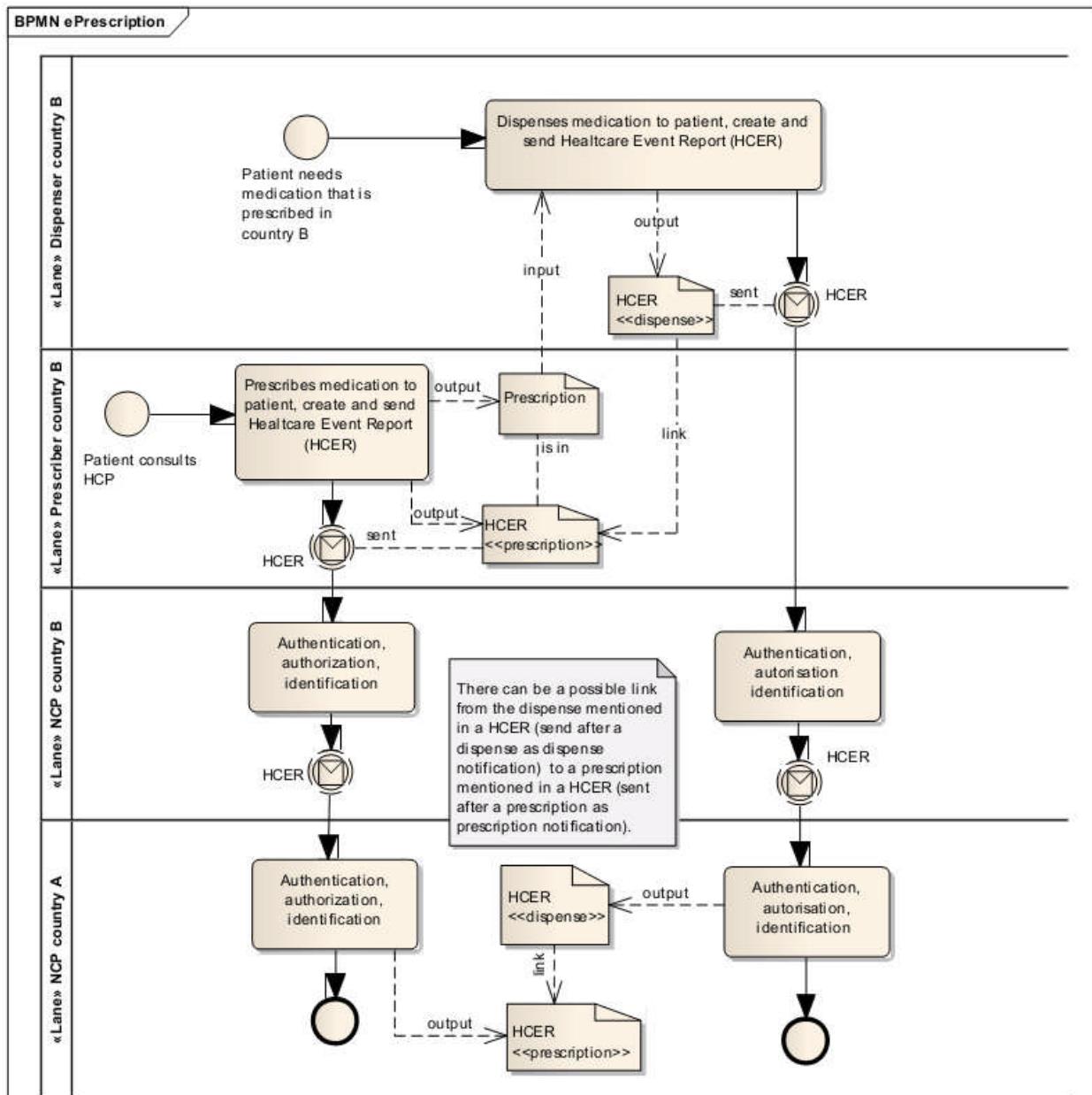
	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Related to e1-TXT-665 Service Pre-requisites

Related to e1-TXT-666 Service Pre-requisites

In this case both medication is prescribed and dispensed in country B, two HCER documents could be sent to country A; one with a report of a prescription being written, and later on a second one with a report of a dispense event based on the prescription. Again, it is up to country A how to handle the HCERs, but the HCER data set offers the possibility to link the dispense data elements in the second HCER with the prescription data elements in the first one (more or less the same way the epSOS phase 1 eDispense can be linked to an epSOS phase 1 ePrescription). This process is depicted in the diagram below.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013



	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.6.1.2.4 e1-TXT-665 Service Pre-requisites

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Related to e1-REQ-3844 MRO Service State Diagram

The service precondition consists of the following elements:

Country A is responsible for keeping the medical information of its own patients up-to-date. These specifications do not make any assumptions on how medical data is managed within a country A.

Country A must provide, maintain and support the NCP supporting communication of the information identified in this section with country B and vice versa and that there must be a chain of trust between system actors in this process. Transaction logging and transport security are available in both country A and B.

Services for identification and authentication of health professionals are available in country B, in a way country B can provide country A with sufficient information to authorize the data access of the health professional of country B.

Patient identification service is available: Country A shall offer the health professional in country B means to validate the identity of the patient.

Legal compliance: Original medical document ownership (owner is both the patient and the entity where the document is stored) and medical / legal validity of transformed document shall be analysed according to the different PN's laws.

Semantic interoperability of structured clinical content: information sent is understandable (in the correct context) for the receiver.

Scalability: The implementation should scale well with respect to the number of documents exchanged

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.1.2.5 e1-REQ-4571 UC.PS.6 Patient Summary Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Actors

The actors involved in the patient summary use cases are the following:

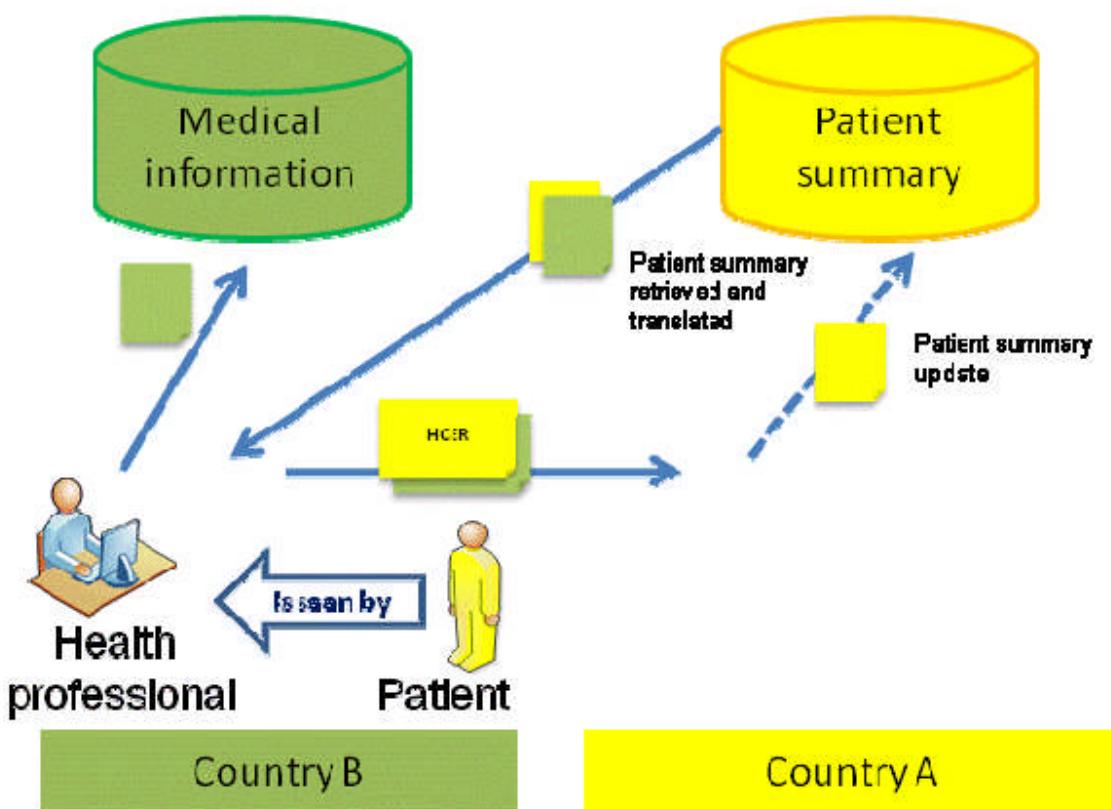
The patient: the patient concerned in these uses cases is always seen by a health professional, either in his/her own country or in country other than his/her home country (country A).

The health professional at the point of care (PoC) in any country, home country or abroad.

Information used

The information used in the Use Cases for patient summary is:

The Patient Summary (PS)



	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The patient visits a health professional in country B:

- 1) The health professional in country B requests the patient summary from country A.
- 2) The health professional in country B records encoded medical information about the patient's treatment event.
- 3) The health professionals sends country A a Healthcare Encounter Report (HCER) to country B
- 4) Based on the information in the HCER, the patient summary in country A can be updated according to the own policies of country A.

3.6.2 e1-FLD-83 Logical Perspective

3.6.2.1 e1-FLD-96 Service Functional Requirements

3.6.2.1.1 e1-REQ-2099 FR01 Utilization of NCP-B Portal for HCER documentation by Health professional in country B

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

As it seems unlikely that any country B healthcare infrastructure offers the possibility to send an HCER document to NCP B, the health professional must be able to fill in a HCER template in the epSOS portal (of the NCP) he/she uses.

3.6.2.1.2 e1-TXT-686 Note

Associated Goals:

Record the information for the HCER

Actors: Health professional, NCP B

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.1.3 e1-REQ-2100 HCER-FR02 Country A is informed of treatment event in country B

Related to e1-REQ-1969 Provisioning of Medical Data by Country B

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Related to e1-REQ-5115 NFR10- Guaranteed delivery

The created HCER must be sent to Country A, respecting the specified requirements in epSOS for sending a document from one PN to another PN (meaning patient identification, HP identification, permission to send and receive medical information about the patient, etc.) Country A must send a confirmation back to Country B after successfully receiving country B's HCER, stating that the document has been received in a good manner. What happens with the information after it is received by NCP A, is out of scope of epSOS.

3.6.2.1.4 e1-TXT-687 Note

Associated Goals:

Inform country A of the treatment event in country B

NCP-B must be informed about the successfully delivered document

Actors: NCPs

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.2 e1-FLD-97 Service ID Management Requirements

3.6.2.2.1 e1-REQ-4991 HP-B Identification and Authentication

Synchronized with e1-REQ-1981 HP-B Identification and Authentication

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

The identity and authenticity of an HP MUST be verified before he can use epSOS cross-border services. Each data access request MUST contain sufficient and verifiable information about (the identity and the role of) the accessory for assessing a country-A national security policy.

3.6.2.2.2 e1-TXT-688 Note

Associated Goals:

To provide security to the process

To ensure that the health professional is legally allowed to perform the functionalities described in this document

Actors: Health professional, NCPs

Preconditions:

Pre-existence of healthcare professional authentication mechanism in country B

Authorization mechanism in country A (based on the informationthat is offered by country B)

3.6.2.2.3 e1-REQ-5077 Patient Identification

Synchronized with e1-REQ-1973 Patient Identification

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

The intended recipient of medical data MUST identify the patient with sufficient accuracy. Medical data MUST only be disclosed after the patient was identified with sufficient accuracy.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

Technical means for patient identification MUST NOT use or disclose medical data about this patient. Patient identifiers SHOULD NOT technically enable any unlawful linkage of the patient's medical data to other sanctioned personal data beyond any legitimate purpose from other domains. If technical means for identity protection (e.g. pseudonymization) are used, these MUST NOT disqualify the responsible parties to lawfully provide the patient access to his/her data. The original identification of the patient MUST NOT rely on the existence of electronic identifiers (eIDs). epSOS use cases MAY define further constraints on the accuracy and means of patient identification for that specific use case (e.g. identification by name considered as insufficient for the 112 use case).

3.6.2.2.4 e1-TXT-689 Note

Associated Goals:

To have certainty of the identity of the patient in both country A as in country B

Actors: Patient, Health professional, NCPs

3.6.2.3 e1-FLD-98 Service Legal Requirements

3.6.2.3.1 e1-REQ-5081 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Related to e1-REQ-2106 HCER-FR06 Information Traceability

Cross-border exchange of medical data MUST be documented in a fully traceable, reconstructable, and seamless fashion.

Cross-border exchange of medical data MUST produce a usable chain of digital evidence that enables both, the patient and his assigned DPA, to pursue, enforce, and proof any assumed or detected violation of the patient's data protection and privacy rights.

The chain of digital evidence MUST disclose the minimum of personal health data required to serve its purpose and MUST be specifically safeguarded against wrongdoing. Part of these safeguards MUST be a protocol that is not accessible to HPs.

Implications:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Audit trails SHOULD be written at both NCPs. For the purpose of data minimization NCP audit trails SHOULD not include medical data but just refer to (and safeguard) respective audit trails within HP systems.

3.6.2.3.2 e1-REQ-2106 HCER-FR06 Information Traceability

Related to e1-REQ-5081 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

The information describing the process and the data involved in the process must be retrievable. This includes information such as the patient, the health professional, the exact place and time where the treatment event took place and all the medical information involved.

3.6.2.3.3 e1-TXT-691 Note

Associated Goals:

Security reasons

Legal reasons

Actors: Health professional, NCPs

Some of this information may not necessarily be contained in the datasets exchanged between countries (as they have been considered maximum datasets).

3.6.2.3.4 e1-REQ-5085 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-1977 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Medical data MUST NOT be disclosed to persons or organization unless they have been authorized by the patient (see »Consent-2; PIN«) and the disclosure is legally or explicitly required for fulfilling the treatment.

Medical data MUST NOT be disclosed to others than healthcare professionals or healthcare professional organizations in any case.

Medical data MUST NOT be transferred to other destinations unless this disclosure has been authorized by the patient or is mandated by national law.

The proper enforcement of the willful disclosure acc. to »consent-2« MUST be controllable and

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

verifiable by the patient.

Implications:

Data MUST be encrypted during transfer and whenever it is stored at (intermediate) nodes outside the trusted environment of an HP (see "IT-Systems directly controlled by HPs").

Depending on how "controllable" and "verifiable" are defined this requirement as well implies a need for secure end-to-end encryption between trusted HP environments.

3.6.2.3.5 e1-REQ-5089 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

The provisioning of medical data for cross-border medical use cases MUST require a willful and documentable act of agreeing by the patient.

This willful act MUST fulfill all requirements of an informed, free consent acc. to country-A legislation. It MUST deliver an appropriate level of data security and privacy for the patient as it is defined in his home country.

This willful act MUST be designed in full anticipation of a cross-border health data exchange scenario.

The respective consent MUST be given in written form and MUST be signed by the patient. A qualified digital signature MAY be used instead of a wet signature.

A country MUST assure that patient data is only accessible if a valid patient consent for data provisioning exists. A country MUST ensure that data is no longer accessible after the respective consent has been revoked or expired.

A HP- B is not required to explicitly verify the existence of a patient's »consent-1« (that was formerly given in country-A) as it is assumed that all epSOS country-A have established secure processes for enforcing the revocation of consents and therefore will not provide data to a country-B unless a valid »consent-1« exists.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.6.2.3.6 e1-REQ-5092 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Triggering a cross-country transfer of medical data MUST require a willful act by the patient.

This willful act MUST express the patient's explicit authorization to allow an identifiable healthcare professional the execution of defined data access operations.

This willful act MUST express the explicit authorization of the patient to transfer medical data to the formerly identified and specifically documented destination.

Countries MAY require that this willful act is documented by an explicit, written and informed consent that is to be signed by the patient.

Implications:

The authorization to perform a specific operation can only be given and documented in country-B (as this authorization requires the identification of both the patient and the HP-B).

Therefore epSOS MUST provide technical means to transmit information about the authorization/PIN to country-A before or while a data access operation is triggered.

3.6.2.3.7 e1-TXT-690 Note

Associated Goals:

Manifesting the legal foundation for a lawful data processing

Granting the patient his specific rights according to data protection regulations

Deciding on whether a certain request for data is legitimated by the consent or not

Actors: Patient, Health professional

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.4 e1-FLD-244 Service Security Requirements

3.6.2.4.1 e1-REQ-5097 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-2206 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

epSOS agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations must be secured and codes of conduct as part of the epSOS Information Governance must be elaborated.

3.6.2.4.2 e1-REQ-5105 Data Integrity

Synchronized with e1-REQ-1978 Data Integrity

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

The integrity of transmitted data MUST be preserved when information is transmitted between different entities (legally or technically defined). It must be verifiable to a data receiver that data has not been damaged, altered or (partially) lost.

3.6.2.4.3 e1-REQ-5119 Data Origin and Data Authenticity

Synchronized with e1-REQ-1984 Data Origin and Data Authenticity

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

The intended recipient of a medical data communication MUST be able to determine the originator and level of authenticity of the medical data received. Information on the identity and authenticity of the data originator that is assigned to the data or its metadata MUST NOT be altered during cross-border transfer.

3.6.2.4.4 e1-REQ-5123 NFR05- Access control

Synchronized with e1-REQ-3880 NFR05- Access control

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

As authorisations involve the existence of a treatment context inside a HCPO, these treatment relationships must be justifiable on demand. The communication partners (origin, destination, and potential facilitators) MUST be known to each other with prior positive verification that all involved partners are authentic (security features to be provided by the means of an identity (subjects, actors, objects) and access management).

3.6.2.4.5 e1-TXT-864 Note

Associated Goals:

For traceability reasons

For security reasons

To assure confidentiality

For Confidentiality and integrity of medical data reasons

To align to the European Data Protection Regulations

3.6.2.5 e1-FLD-100 Service Clinical Requirements

3.6.2.5.1 e1-REQ-2111 HCER-FR09 Link HCERs

Related to e1-REQ-1987 Relationships among Documents and/or Document Entries

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Country A MUST be able to relate the prescription and dispense to each other to see if a prescription actually has been dispensed. In country A it should be possible to relate the information of one HCER with another HCER.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.5.2 e1-TXT-693 Note

Associated Goals:

Link the dispensed information to the prescription

To have information complete and reliable

Actors: NCP A, NCP B

3.6.2.5.3 e1-REQ-5124 Minimum and Maximum Data Sets

Synchronized with e1-REQ-1986 Minimum and Maximum Data Sets

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Every PN MUST provide means that enable an HP IT-System to properly translate, display and process mandatory data entries within epSOS documents. Every PN SHOULD provide means that enable an HP IT-System to properly translate, display and process optional data entries within epSOS documents.

PN MAY define additional data entries within epSOS documents as long as this does not violate the defined pivot schema. PN that receive such extended documents MAY ignore all data elements not defined by epSOS.

3.6.2.5.4 e1-TXT-692 Note

Associated Goals:

To ensure that sent data does reach country A in a good manner as much as possible

Actors: NCP A

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.5.5 e1-REQ-5126 Peering Original Document

Synchronized with e1-REQ-1988 Peering Original Document

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Whenever original data is transcoded/translated for the purpose of cross-border document sharing, the receiver of that data MUST be enabled by epSOS to view that data without transcoding/translation, too. epSOS use case specifications MAY define default behaviors and constraints for peering original documents.

3.6.2.5.6 e1-TXT-694 Note

Associated goals:

For safety reasons. It is possible that for instance a brand name of a medicine is going to be changed in case of a prescription/dispense

Traceability reasons

Actors: NCPs

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.6 e1-FLD-101 Service Semantic Requirements

3.6.2.6.1 e1-REQ-5099 Structured Information and Semantic Compliance

Synchronized with e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

epSOS MUST define the structure and semantics of all document types which are required to be shared cross-border within epSOS use cases (pivot schema and common terminologies).

It is the responsibility of each PN to preserve the semantics of original data when this is transformed and transcoded into the common epSOS format as defined for the respective document type. Transformation services within a country and epSOS semantic services should guarantee the smoothest semantic transformation, keeping the meaning and the value of the source document, considering the liability for the transformation, and assuring the reproducibility of the semantic transformation.

3.6.2.7 e1-FLD-102 Service Usability and Data Presentation Requirements

3.6.2.7.1 e1-REQ-5127 Semantic Interoperability of Structured Clinical Content

Synchronized with e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Medical information shared among countries MUST be understandable (in the correct context) for the receiver. HP-B MUST be enabled to view and/or process medical documents encoded in a way that best matches the document structure and clinical terms that are commonly used in country-B.

Implications:

epSOS MUST provide semantic services that allow for translation/mapping of clinical terms. epSOS SHOULD use a common pivot schema and terminology set in order to limit the number of mappings that have to be defined and maintained.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.7.2 e1-TXT-848 Note

Associated Goals:

Provide ease of processing incoming data for Country A.

To provide the health professional with the necessary information and in a manner he is used to.

Guarantee the safety of the patient through a proper understanding of the received information

Actors: NCPs

Precondition:

It has to be known to NCP-B that it can and is allowed to send the HCER to NCP-A

3.6.2.8 e1-FLD-103 Service Non-functional Requirements: Service Level Requirements

3.6.2.8.1 e1-REQ-2120 HCER-NFR01 Service Availability

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Synchronized with e1-REQ-3850 HCER-NFR01 Service Availability

Every event that causes unavailability MUST be analysed. Each service interruption MUST be detected as soon as possible. The origin of the failure (health information system, National Contact Point system, central broker ...) MUST be explained.

When there is a transition to a degraded mode, the suitable alerts MUST be defined and particularly the procedure for using a degraded mode.

In this respect, a special focus on the procedure for using degraded mode should be set on cases of a patient emergency such as an emergency mode (like a collapsed patient or an accident where the patient is severely injured).

The availability of the system MUST be measured in order to evaluate the performance of the system.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.6.2.8.2 e1-TXT-849 Note

Availability means the property of being accessible and usable upon demand by an authorized entity (see definition ISO 7498-2:1989). There are different causes for technical unavailability (of communication, National Contact Points, local systems...) of the epSOS LSP service as:

failure

unplanned stop (bug, random error)

partial planned stop (not optimal running)

planned stop (maintenance, update)

Associated Goals:

Continuous 24h a day, 7 days a week availability of the service

3.6.2.8.3 e1-REQ-2121 HCER-NFR02 Response time

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Synchronized with e1-REQ-4583 HCER-NFR02 Response time

Synchronized with e1-REQ-5109 HCER-NFR02 Response time

The system SHOULD provide an average end to end response time within 5 seconds.

The average end to end response time MUST NOT be more than 10 seconds.

3.6.2.8.4 e1-TXT-695 Note

Associated Goals:

Information has to travel from one country to another. An acceptable time response not only applies to the receipt of information, but also to the identification and authentication of health professional and patient

The system should provide an acceptable end-to-end response time, not degrading or delaying the already existing services because the patient is waiting while the system accesses and shows the required information

The access times should be tested continually by the system to give the user some idea of what to expect

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.8.5 e1-REQ-5095 NFR09- Trust between countries

Synchronized with e1-REQ-4564 NFR09- Trust between countries

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

All the countries involved in the project are integrated into one circle of trust (technical). An agreed framework for creating trust MUST be established, encompassing processes and procedures for critical data protection, privacy and confidentiality issues as well as mechanisms for their audit. Such issues include, but are not limited to:

- Identification, authentication and authorisation mechanisms
- Security and trust mechanisms
- Recording and exchanging patient consent

3.6.2.8.6 e1-TXT-846 Note

Associated Goals:

To enable the exchange of information between countries.

To avoid having to identify all professionals and institutions from a foreign country in the country of origin. On the one hand, each HP will be unequivocally identified and authenticated in his local system and must be identified based on his/her role/profile. On the other hand, Health Care Provider Organisation provides HP a status, a function, an authentication from which the HP trust is derived. Furthermore, Health Authorities Institutions assign and assure the status, the role, and sometimes the authentication of HP .

3.6.2.8.7 e1-REQ-5115 NFR10- Guaranteed delivery

Related to e1-REQ-2100 HCER-FR02 Country A is informed of treatment event in country B

Synchronized with e1-REQ-3885 NFR10- Guaranteed delivery

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

When information is sent from one country to another, it MUST be assured that the information has been properly received by the user in the receiver country.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.8.8 e1-TXT-859 Note

Associated Goals:

security reasons

to check that the ePrescription service has been properly completed

3.6.2.8.9 e1-REQ-5117 NFR12- Supervision services

Synchronized with e1-REQ-3887 NFR12- Supervision services

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

A service MUST be put in place to detect all the technical exceptions and to check and monitor the performance of the service (time response, communications...).

3.6.2.8.10 e1-TXT-861 Note

Associated Goals:

To assure the availability and to avoid degradation of the service

3.6.2.9 e1-FLD-104 Additional Architecture NCP/Central Service Requirements

3.6.2.9.1 e1-REQ-2123 HCER-NFR03 New document type

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

New document type Healthcare Encounter Report MUST be able to be sent by country B.

3.6.2.9.2 e1-TXT-696 Note

Associated Goals:

The HCER is a newly introduced document type in epSOS phase 2. National Contact Points and Central Services need to be adjusted to be able to handle this.

Actors: NCPs

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.6.2.9.3 e1-REQ-2124 HCER-FR14 Forwarding HCER

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

HCERs received by NCP-A MUST NOT be stored at NCP-A.

NCP-A MAY forward the HCERs to health professionals (information system) or the personal health record of the patient.

3.6.2.9.4 e1-TXT-697 Note

Associated Goals:

Having up-to-date information in country A.

Not making country B responsible for the availability of healthcare information on foreign patients.

Not making the NCP responsible for the availability of medical data

Actors: NCP A, Healthcare ICT infrastructure of country B

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

3.7 e1-FLD-63 Prescription Extended Service Specification: Medication Related Overview

3.7.1 e1-FLD-84 Conceptual Perspective

3.7.1.1 e1-FLD-248 Information Dimension

3.7.1.1.1 e1-REQ-5139 About Patient Identification in the ePrescription

Synchronized with e1-REQ-1668 About Patient Identification in the ePrescription

Variable	Definitions	MS: Minimum Optional	Comments	Example
Given Name	The Name of the patient	Yes	This field can contain more than one element	Marta
Family Name/Surname	The surname/s of the patient	Yes	This field can contain more than one element	Español Smith
Gender	The gender of the patient	Yes		Male/female/unknown
Birth date	Date of birth	Yes	This field may contain only the year	01/01/2009
Regional/National Health Id	If the patient has a regional or national Health Identification	Yes	This field is required by some national laws	
Social/Insurance Number		Yes	If a patient has both, national/regional ID and Social/Insurance number, only the regional/national Health Id is required by law. If the only identification the patient has is the Social/insurance number, then	

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

			this one is considered as the regional/national Health Id. This field is required by some national laws.	
--	--	--	--	--

3.7.1.1.2 e1-REQ-5145 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-1669 About HP Prescriber Identification in the ePrescription

Variable	Definitions	MS: Minimum Max: maximum	Comments	Example
Given Name	The Name of the Prescriber	MS	This field can contain more than one element	Marta
Family name/surname	The surname/s of the Prescriber	MS	This field can contain more than one element	Español Smith
HP Id number	The identification of the person as HP	MS		12345
Profession		MS		Physician
Specialist		Max		Dermatologist
Prescriber Facility Address:	The place (complete address) where the prescriber made the prescription		This is not a field but a block of information made up of the following fields. This might not be in the dataset but this information needs to be available for the process traceability (FR20)	e.g., Los Bermejales Health Care Centre. Alemania St. Seville, 41018. Spain

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Name of the Facility		Max		For instance, the name of the building: Los Bermejales
Street Address		Max		Alemania Street
City		Max		Seville
State or Province		Max		Seville
Zip or Postal Code		Max		41018
Telephone		Max		+34 954123123
Contact email of the centre or of the prescriber		Max		losbermejaleshealthcentre@xxx.es
Country	The country where the prescription was made	MS	The dispenser needs to know the country where he is consulting the information from	Spain
Prescriber Organization:			This is not a field but a block of information made up of the following fields. This might not be in the dataset but this information needs to be available for the process traceability (FR20)	
Organization Name		Max		e.g. Andalusia Health Service
Organization Identifier		Max	This field can be numbers and/or letters	123458xfs

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.7.1.2 e1-FLD-135 Computational Dimension

3.7.1.2.1 e1-REQ-4573 UC.MED.1 Medication Related Overview available for dispenser in country B

Related to e1-REQ-3844 MRO Service State Diagram

Description

A patient from country A is visiting country B. The patient has a prescription that is not fully dispensed yet. The patient needs medication to be dispensed, based upon this prescription. The patient goes to a pharmacy in country B. The pharmacy in country B obtains, from country A, the medication history of the patient which includes the unfulfilled prescription and the medication related overview. The medication related overview is obtained in a form and richness common in country A (how country A normally informs a pharmacist). The pharmacist checks the medication to be dispensed against the medication related overview to check for possible adverse reactions and / or other unwanted effects. When the pharmacist can assume that medication can be safely and legally dispensed, the medication is handed to the patient or the person representing the patient (e.g. a family member). The pharmacist in country B makes the dispensation information available, which then is transferred to the home country for inclusion into the medication history in country A, and for updating the status of the prescription in country A, i.e. lowering the remaining amount of possible dispenses from that prescription.

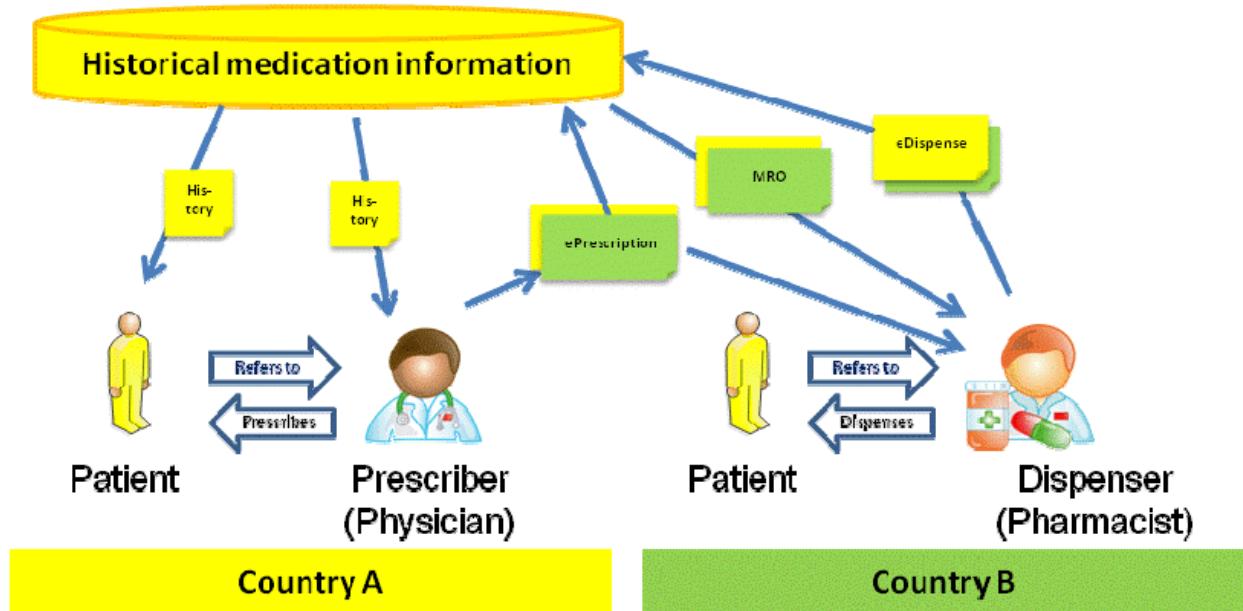
Actors

The actors involved in these Use Cases are:

The patient: the patient concerned in these cases is always seen by a health professional, either in his/her own country or in country other than his/her home country (country A).

The health professional at the point of care (PoC) in any country, home country or abroad.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013



3.7.1.2.2 e1-REQ-4575 UC.MED.2 Medicine newly prescribed in country B

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3844 MRO Service State Diagram

Description

A patient from country A is visiting country B. The patient needs care and visits a physician in country B. The physician and the patient conclude that the patient needs medication. The physician in country B consults the medication history (i.e. medication related overview) from country A, and based upon that history and the current situation (illness) of the patient, issues a prescription. That prescription is sent to country A for inclusion into the medication history in country A, for future reference. The patient goes to a pharmacy in country B. The pharmacy in country B obtains, from country A, the medication history of the patient which includes the unfulfilled prescription and the medication related overview. The medication related overview is obtained in a form and richness common in country A (how country A normally informs a pharmacist). The pharmacist obtains the electronic prescription from the physician in country B, through the regular Country B procedure. The pharmacist checks the medication to be dispensed against the medication related overview, to check for possible adverse reactions and / or other unwanted effects. When the pharmacist can assume that medication can be safely and legally dispensed, the medication is handed to the patient or the person representing the patient (e.g. a family member). The pharmacist in country B makes the dispense information available in electronic form, which then is transferred to the home country for inclusion into the

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

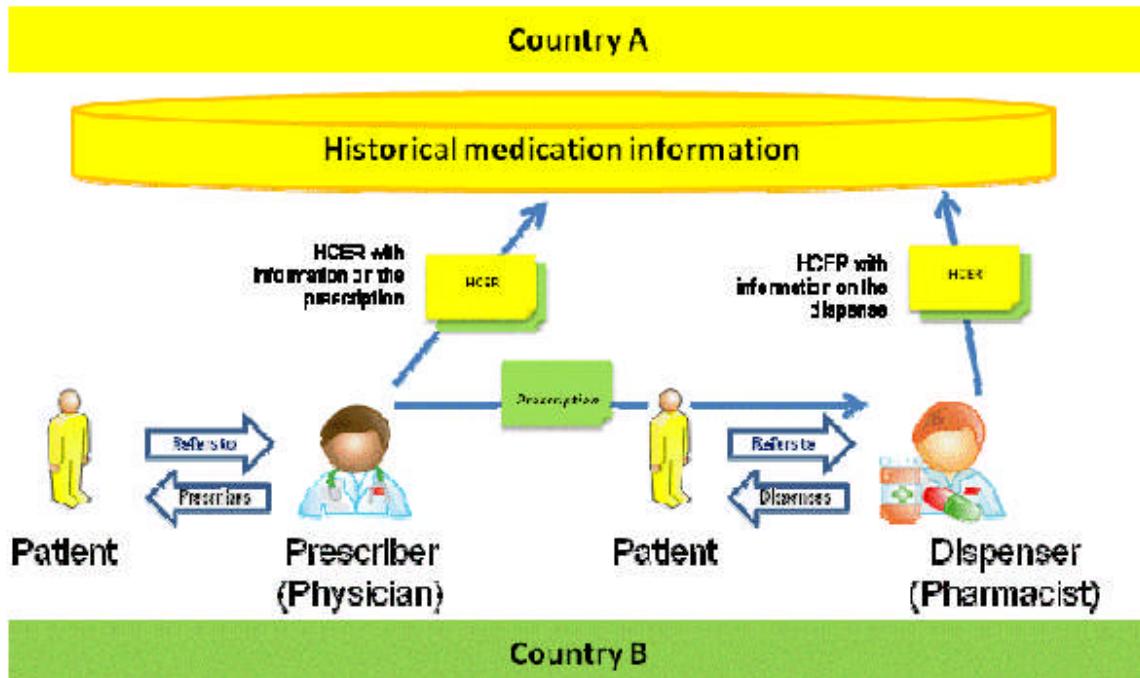
medication history in country A.

Actors

The actors involved in these Use Cases are:

The patient: the patient concerned in these uses cases is always seen by a health professional, either in his/her own country or in country other than his/her home country (country A).

The health professional at the point of care (PoC) in any country, home country or abroad.



	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.7.1.2.3 e1-REQ-3844 MRO Service State Diagram

Related to e1-REQ-5093 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-5106 Data Integrity

Related to e1-REQ-5121 Data Origin and Data Authenticity

Related to e1-REQ-5076 HP-B Identification and Authentication

Related to e1-REQ-5098 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-5128 Minimum and Maximum Data Sets

Related to e1-REQ-2126 MRO-FR01 Country A offers access to medication related information

Related to e1-REQ-2127 MRO-FR02 Health professional in country B requests the MRO

Related to e1-REQ-2133 MRO-FR06 Information Traceability

Related to e1-REQ-2149 MRO-NFR03 New document type

Related to e1-REQ-5110 NFR05- Access control

Related to e1-REQ-5078 Patient Identification

Related to e1-REQ-5129 Peering Original Document

Related to e1-REQ-5102 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-5101 Structured Information and Semantic Compliance

Related to e1-REQ-5082 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-4573 UC.MED.1 Medication Related Overview available for dispenser in country B

Related to e1-REQ-4575 UC.MED.2 Medicine newly prescribed in country B

Related to e1-REQ-5086 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-5090 Willful Provisioning of Data (»Consent-1«)

Related to e1-TXT-664 Service Pre-requisites

Related to e1-TXT-665 Service Pre-requisites

Related to e1-TXT-666 Service Pre-requisites

MRO as addition to the epSOS phase 1 e Prescription

In a situation in which the patient has prescribed medicine in country A and wants these to be dispensed in country B with the use of the epSOS phase 1 eP service that is made up of electronic prescribing and electronic dispensing, the MRO service might give useful information for patient safety to the dispensing health professional in country B.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

MRO as addition to a country B prescription

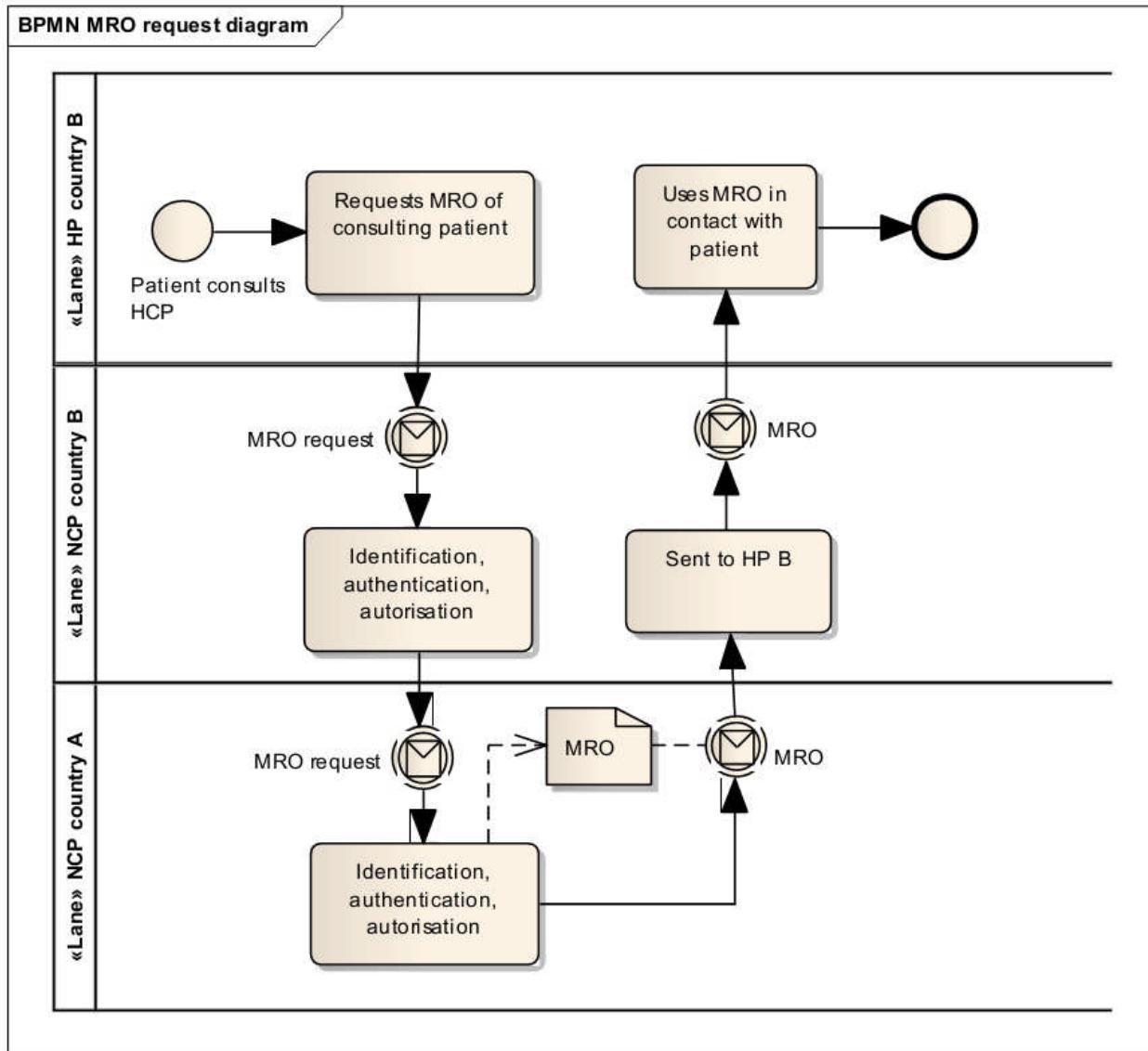
In a common use case, in which the patient from country A gets medication prescribed and dispensed by health professionals in country B, the MRO could give useful information for

patient safety to the prescribing and dispensing health professionals in country B. A prescriber in country B could access the patient summary as well as the MRO, but note that there is

overlap between the PS and the MRO, as some medication information in the MRO can also be part of the PS.

Below is shown the state diagram of the process of requesting the MRO of country A by a health professional in country B.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013



3.7.1.2.4 e1-TXT-666 Service Pre-requisites

Related to e1-REQ-3843 HCER Service State Diagram ePrescription Extension

Related to e1-REQ-3842 HCER Service State Diagram Patient Summary Extension

Related to e1-REQ-3844 MRO Service State Diagram

The service precondition consists of the following elements:

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Country A is responsible for keeping the medical information of its own patients up-to-date. These specifications do not make any assumptions on how medical data is managed within a country A.

Country A must provide, maintain and support the NCP supporting communication of the information identified in this section with country B and vice versa and that there must be a chain of trust between system actors in this process. Transaction logging and transport security are available in both country A and B.

Services for identification and authentication of health professionals are available in country B, in a way country B can provide country A with sufficient information to authorize the data access of the health professional of country B.

Patient identification service is available: Country A shall offer the health professional in country B means to validate the identity of the patient.

Legal compliance: Original medical document ownership (owner is both the patient and the entity where the document is stored) and medical / legal validity of transformed document shall be analysed according to the different PN's laws.

Semantic interoperability of structured clinical content: information sent is understandable (in the correct context) for the receiver.

Scalability: The implementation should scale well with respect to the number of documents exchanged

3.7.2 e1-FLD-85 Logical Perspective

3.7.2.1 e1-FLD-105 Service Functional Requirements

3.7.2.1.1 e1-REQ-2126 MRO-FR01 Country A offers access to medication related information

Related to e1-REQ-3844 MRO Service State Diagram

An overview of all relevant and available information needed in the medication process MUST be available for request by an health professional in country B via the MRO service.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.7.2.1.2 e1-TXT-698 Note

Associated Goals:

Patient safety when prescribing, dispensing or administering medication in country B

Actors: NCP A, Health professionals (information systems) in country A

3.7.2.1.3 e1-REQ-2127 MRO-FR02 Health professional in country B requests the MRO

Related to e1-REQ-3844 MRO Service State Diagram

Via the NCP of country B, a health professional MUST be able to request the MRO of a foreign patient at the MRO service of the patient's country of affiliation (country A).

3.7.2.1.4 e1-TXT-699 Note

Associated Goals:

Patient safety when prescribing, dispensing or administering
medication in country B

Actors: NCPs, Health professional in country B

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.7.2.2 e1-FLD-106 Service ID Management Requirements

3.7.2.2.1 e1-REQ-5076 HP-B Identification and Authentication

Synchronized with e1-REQ-1981 HP-B Identification and Authentication

Related to e1-REQ-3844 MRO Service State Diagram

The identity and authenticity of an HP MUST be verified before he can use epSOS cross-border services. Each data access request MUST contain sufficient and verifiable information about (the identity and the role of) the accessory for assessing a country-A national security policy.

3.7.2.2.2 e1-TXT-839 Note

Associated Goals:

To provide security to the process

To ensure that the health professional is legally allowed to perform the functionalities described in this document

Actors: Health professional, NCPs

Preconditions:

Pre-existence of healthcare professional authentication mechanism in country B

Authorization mechanism in country A (based on the informationthat is offered by country B)

3.7.2.2.3 e1-REQ-5078 Patient Identification

Synchronized with e1-REQ-1973 Patient Identification

Related to e1-REQ-3844 MRO Service State Diagram

The intended recipient of medical data MUST identify the patient with sufficient accuracy. Medical data MUST only be disclosed after the patient was identified with sufficient accuracy.

Technical means for patient identification MUST NOT use or disclose medical data about this patient. Patient identifiers SHOULD NOT technically enable any unlawful linkage of the patient's medical data to other sanctioned personal data beyond any legitimate purpose from other domains. If technical means for identity protection (e.g. pseudonymization) are used, these MUST NOT disqualify the responsible parties to lawfully provide the patient access to his/her

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

data. The original identification of the patient MUST NOT rely on the existence of electronic identifiers (eIDs). epSOS use cases MAY define further constraints on the accuracy and means of patient identification for that specific use case (e.g. identification by name considered as insufficient for the 112 use case).

3.7.2.2.4 e1-TXT-840 Note

Associated Goals:

To have certainty of the identity of the patient in both country A as in country B

Actors: Patient, Health professional, NCPs

3.7.2.3 e1-FLD-107 Service Legal Requirements

3.7.2.3.1 e1-REQ-5082 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-3844 MRO Service State Diagram

Related to e1-REQ-2133 MRO-FR06 Information Traceability

Cross-border exchange of medical data MUST be documented in a fully traceable, reconstructable, and seamless fashion.

Cross-border exchange of medical data MUST produce a usable chain of digital evidence that enables both, the patient and his assigned DPA, to pursue, enforce, and proof any assumed or detected violation of the patient's data protection and privacy rights.

The chain of digital evidence MUST disclose the minimum of personal health data required to serve its purpose and MUST be specifically safeguarded against wrongdoing. Part of these safeguards MUST be a protocol that is not accessible to HPs.

Implications:

Audit trails SHOULD be written at both NCPs. For the purpose of data minimization NCP audit trails SHOULD not include medical data but just refer to (and safeguard) respective audit trails within HP systems.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.7.2.3.2 e1-REQ-2133 MRO-FR06 Information Traceability

Related to e1-REQ-5082 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-3844 MRO Service State Diagram

The information describing the process and the data involved in the process must be retrievable. This should include information such as the health professional, the exact place and time where the prescription was made, the identification of the pharmacy where the medicine was dispensed, the health professional that dispensed it, if there was a substitution, the original prescription, the translation of the prescription from country A to country B, the epSOS format Specifically, all information that has been considered as minimum and maximum in the prescription and dispensed medicine datasets.

3.7.2.3.3 e1-TXT-842 Note

Associated Goals:

Security reasons

Legal reasons

Actors: Health professional, NCPs

Some of this information may not necessarily be contained in the datasets exchanged between countries (as they have been considered maximum datasets).

3.7.2.3.4 e1-REQ-5086 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-1977 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-3844 MRO Service State Diagram

Medical data MUST NOT be disclosed to persons or organization unless they have been authorized by the patient (see »Consent-2; PIN«) and the disclosure is legally or explicitly required for fulfilling the treatment.

Medical data MUST NOT be disclosed to others than healthcare professionals or healthcare professional organizations in any case.

Medical data MUST NOT be transferred to other destinations unless this disclosure has been authorized by the patient or is mandated by national law.

The proper enforcement of the willful disclosure acc. to »consent-2« MUST be controllable and verifiable by the patient.

Implications:

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Data MUST be encrypted during transfer and whenever it is stored at (intermediate) nodes outside the trusted environment of an HP (see "IT-Systems directly controlled by HPs").

Depending on how "controllable" and "verifiable" are defined this requirement as well implies a need for secure end-to-end encryption between trusted HP environments.

3.7.2.3.5 e1-REQ-5090 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-3844 MRO Service State Diagram

The provisioning of medical data for cross-border medical use cases MUST require a willful and documentable act of agreeing by the patient.

This willful act MUST fulfill all requirements of an informed, free consent acc. to country-A legislation. It MUST deliver an appropriate level of data security and privacy for the patient as it is defined in his home country.

This willful act MUST be designed in full anticipation of a cross-border health data exchange scenario.

The respective consent MUST be given in written form and MUST be signed by the patient. A qualified digital signature MAY be used instead of a wet signature.

A country MUST assure that patient data is only accessible if a valid patient consent for data provisioning exists. A country MUST ensure that data is no longer accessible after the respective consent has been revoked or expired.

A HP- B is not required to explicitly verify the existence of a patient's »consent-1« (that was formerly given in country-A) as it is assumed that all epSOS country-A have established secure processes for enforcing the revocation of consents and therefore will not provide data to a country-B unless a valid »consent-1« exists.

3.7.2.3.6 e1-REQ-5093 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-3844 MRO Service State Diagram

Triggering a cross-country transfer of medical data MUST require a willful act by the patient.

This willful act MUST express the patient's explicit authorization to allow an identifiable healthcare professional the execution of defined data access operations.

This willful act MUST express the explicit authorization of the patient to transfer medical data to the formerly identified and specifically documented destination.

Countries MAY require that this willful act is documented by an explicit, written and informed consent that is to be signed by the patient.

Implications:

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

The authorization to perform a specific operation can only be given and documented in country-B (as this authorization requires the identification of both the patient and the HP-B).

Therefore epSOS MUST provide technical means to transmit information about the authorization/PIN to country-A before or while a data access operation is triggered.

3.7.2.3.7 e1-TXT-844 Note

Associated Goals:

Manifesting the legal foundation for a lawful data processing

Granting the patient his specific rights according to data protection regulations

Deciding on whether a certain request for data is legitimated by the consent or not

Actors: Patient, Health professional

3.7.2.4 e1-FLD-245 Service Security Requirements

3.7.2.4.1 e1-REQ-5098 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-2206 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-3844 MRO Service State Diagram

epSOS agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations must be secured and codes of conduct as part of the epSOS Information Governance must be elaborated.

3.7.2.4.2 e1-REQ-5106 Data Integrity

Synchronized with e1-REQ-1978 Data Integrity

Related to e1-REQ-3844 MRO Service State Diagram

The integrity of transmitted data MUST be preserved when information is transmitted between different entities (legally or technically defined). It must be verifiable to a data receiver that data has not been damaged, altered or (partially) lost.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.7.2.4.3 e1-REQ-5110 NFR05- Access control

Synchronized with e1-REQ-3880 NFR05- Access control

Related to e1-REQ-3844 MRO Service State Diagram

As authorisations involve the existence of a treatment context inside a HCPO, these treatment relationships must be justifiable on demand. The communication partners (origin, destination, and potential facilitators) MUST be known to each other with prior positive verification that all involved partners are authentic (security features to be provided by the means of an identity (subjects, actors, objects) and access management).

3.7.2.4.4 e1-TXT-854 Note

Associated Goals:

For traceability reasons

For security reasons

To assure confidentiality

For Confidentiality and integrity of medical data reasons

To align to the European Data Protection Regulations

3.7.2.4.5 e1-REQ-5121 Data Origin and Data Authenticity

Synchronized with e1-REQ-1984 Data Origin and Data Authenticity

Related to e1-REQ-3844 MRO Service State Diagram

The intended recipient of a medical data communication MUST be able to determine the originator and level of authenticity of the medical data received. Information on the identity and authenticity of the data originator that is assigned to the data or its metadata MUST NOT be altered during cross-border transfer.

3.7.2.4.6 e1-TXT-856 Note

Associated Goals:

To guarantee that the issuer of the information exchanged cannot refuse that the issuance has taken place

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.7.2.5 e1-FLD-109 Service Clinical Requirements

3.7.2.5.1 e1-REQ-5128 Minimum and Maximum Data Sets

Synchronized with e1-REQ-1986 Minimum and Maximum Data Sets

Related to e1-REQ-3844 MRO Service State Diagram

Every PN MUST provide means that enable an HP IT-System to properly translate, display and process mandatory data entries within epSOS documents. Every PN SHOULD provide means that enable an HP IT-System to properly translate, display and process optional data entries within epSOS documents.

PN MAY define additional data entries within epSOS documents as long as this does not violate the defined pivot schema. PN that receive such extended documents MAY ignore all data elements not defined by epSOS.

3.7.2.5.2 e1-TXT-701 Note

Associated Goals:

To ensure that sent data does reach country B in a good manner as much as possible

Actors: National infrastructure country B

3.7.2.5.3 e1-REQ-5129 Peering Original Document

Synchronized with e1-REQ-1988 Peering Original Document

Related to e1-REQ-3844 MRO Service State Diagram

Whenever original data is transcoded/translated for the purpose of cross-border document sharing, the receiver of that data MUST be enabled by epSOS to view that data without transcoding/translation, too. epSOS use case specifications MAY define default behaviors and constraints for peering original documents.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

3.7.2.5.4 e1-TXT-702 Note

Associated Goals:

Show original information. The MRO is not the source on which dispenses in country B may be done. The health professional needs a valid prescription for this (epSOS ePrescription or local prescription)

Actors: NCPs

3.7.2.6 e1-FLD-110 Service Semantic Requirements

3.7.2.6.1 e1-REQ-5101 Structured Information and Semantic Compliance

Synchronized with e1-REQ-1983 Structured Information and Semantic Compliance

Related to e1-REQ-3844 MRO Service State Diagram

epSOS MUST define the structure and semantics of all document types which are required to be shared cross-border within epSOS use cases (pivot schema and common terminologies).

It is the responsibility of each PN to preserve the semantics of original data when this is transformed and transcoded into the common epSOS format as defined for the respective document type. Transformation services within a country and epSOS semantic services should guarantee the smoothest semantic transformation, keeping the meaning and the value of the source document, considering the liability for the transformation, and assuring the reproducibility of the semantic transformation.

3.7.2.6.2 e1-TXT-703 Note

Associated Goals:

International standardization to ensure semantic understanding between users of communicating systems.

Safety reasons

Actors: NCPs, Health professional

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.7.2.7 e1-FLD-111 Service Usability and Data Presentation Requirements

3.7.2.7.1 e1-REQ-5102 Semantic Interoperability of Structured Clinical Content

Synchronized with e1-REQ-1982 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-3844 MRO Service State Diagram

Medical information shared among countries MUST be understandable (in the correct context) for the receiver. HP-B MUST be enabled to view and/or process medical documents encoded in a way that best matches the document structure and clinical terms that are commonly used in country-B.

Implications:

epSOS MUST provide semantic services that allow for translation/mapping of clinical terms. epSOS SHOULD use a common pivot schema and terminology set in order to limit the number of mappings that have to be defined and maintained.

3.7.2.8 e1-FLD-112 Service Non-functional Requirements: Service Level Requirements

3.7.2.8.1 e1-REQ-3850 HCER-NFR01 Service Availability

Synchronized with e1-REQ-2120 HCER-NFR01 Service Availability

Every event that causes unavailability MUST be analysed. Each service interruption MUST be detected as soon as possible. The origin of the failure (health information system, National Contact Point system, central broker ...) MUST be explained.

When there is a transition to a degraded mode, the suitable alerts MUST be defined and particularly the procedure for using a degraded mode.

In this respect, a special focus on the procedure for using degraded mode should be set on cases of a patient emergency such as an emergency mode (like a collapsed patient or an accident where the patient is severely injured).

The availability of the system MUST be measured in order to evaluate the performance of the system.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.7.2.8.2 e1-TXT-851 Note

Availability means the property of being accessible and usable upon demand by an authorized entity (see definition ISO 7498-2:1989). There are different causes for technical unavailability (of communication, National Contact Points, local systems...) of the epSOS LSP service as:

failure

unplanned stop (bug, random error)

partial planned stop (not optimal running)

planned stop (maintenance, update)

Associated Goals:

Continuous 24h a day, 7 days a week availability of the service

3.7.2.8.3 e1-REQ-4583 HCER-NFR02 Response time

Synchronized with e1-REQ-2121 HCER-NFR02 Response time

The system SHOULD provide an average end to end response time within 5 seconds.
The average end to end response time MUST NOT be more than 10 seconds.

3.7.2.8.4 e1-TXT-705 Note

Associated Goals:

Information has to travel from one country to another. An acceptable time response not only applies to the receipt of information, but also to the identification and authentication of health professional and patient

The system should provide an acceptable end-to-end response time, not degrading or delaying the already existing services because the patient is waiting while the system accesses and shows the required information

The access times should be tested continually by the system to give the user some idea of what to expect

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.7.2.8.5 e1-REQ-5096 NFR09- Trust between countries

Synchronized with e1-REQ-4564 NFR09- Trust between countries

All the countries involved in the project are integrated into one circle of trust (technical). An agreed framework for creating trust MUST be established, encompassing processes and procedures for critical data protection, privacy and confidentiality issues as well as mechanisms for their audit. Such issues include, but are not limited to:

- Identification, authentication and authorisation mechanisms
- Security and trust mechanisms
- Recording and exchanging patient consent

3.7.2.8.6 e1-TXT-847 Note

Associated Goals:

To enable the exchange of information between countries.

To avoid having to identify all professionals and institutions from a foreign country in the country of origin. On the one hand, each HP will be unequivocally identified and authenticated in his local system and must be identified based on his/her role/profile. On the other hand, Health Care Provider Organisation provides HP a status, a function, an authentication from which the HP trust is derived. Furthermore, Health Authorities Institutions assign and assure the status, the role, and sometimes the authentication of HP .

3.7.2.8.7 e1-REQ-5116 NFR10- Guaranteed delivery

Synchronized with e1-REQ-3885 NFR10- Guaranteed delivery

When information is sent from one country to another, it MUST be assured that the information has been properly received by the user in the receiver country.

3.7.2.8.8 e1-TXT-860 Note

Associated Goals:

security reasons

to check that the ePrescription service has been properly completed

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.7.2.8.9 e1-REQ-5130 NFR12- Supervision services

Synchronized with e1-REQ-3887 NFR12- Supervision services

A service MUST be put in place to detect all the technical exceptions and to check and monitor the performance of the service (time response, communications....).

3.7.2.8.10 e1-TXT-865 Note

Associated Goals:

To assure the availability and to avoid degradation of the service

3.7.2.9 e1-FLD-113 Additional Architecture NCP/Central Service Requirements

3.7.2.9.1 e1-REQ-2149 MRO-NFR03 New document type

Related to e1-REQ-3844 MRO Service State Diagram

New document type Medication Related Overview MUST be able to be requested by country B.

3.7.2.9.2 e1-TXT-706 Note

Associated Goals:

The Medication Related Overview is a newly introduced document type in epSOS phase 2. National Contact Points and Central Services need to be adjusted to be able to handle this

Actors: NCPs

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

3.8 e1-FLD-62 112 Additional Service Specification

3.8.1 e1-FLD-86 Conceptual Perspective

3.8.1.1 e1-FLD-249 Information Dimension

3.8.1.1.1 e1-REQ-5140 About Patient Identification in the ePrescription

Synchronized with e1-REQ-1668 About Patient Identification in the ePrescription

Variable	Definitions	MS: Minimum Optional	Comments	Example
Given Name	The Name of the patient	Yes	This field can contain more than one element	Marta
Family Name/Surname	The surname/s of the patient	Yes	This field can contain more than one element	Español Smith
Gender	The gender of the patient	Yes		Male/female/unknown
Birth date	Date of birth	Yes	This field may contain only the year	01/01/2009
Regional/National Health Id	If the patient has a regional or national Health Identification	Yes	This field is required by some national laws	
Social/Insurance Number		Yes	If a patient has both, national/regional ID and Social/Insurance number, only the regional/national Health Id is required by law. If the only identification the patient has is the Social/insurance number, then this one is considered as the	

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

			regional/national Health Id. This field is required by some national laws.	
--	--	--	--	--

3.8.1.1.2 e1-REQ-5146 About HP Prescriber Identification in the ePrescription

Synchronized with e1-REQ-1669 About HP Prescriber Identification in the ePrescription

Variable	Definitions	MS: Minimum Max: maximum	Comments	Example
Given Name	The Name of the Prescriber	MS	This field can contain more than one element	Marta
Family name/surname	The surname/s of the Prescriber	MS	This field can contain more than one element	Español Smith
HP Id number	The identification of the person as HP	MS		12345
Profession		MS		Physician
Specialist		Max		Dermatologist
Prescriber Facility Address:	The place (complete address) where the prescriber made the prescription		<p>This is not a field but a block of information made up of the following fields.</p> <p>This might not be in the dataset but this information needs to be available for the process traceability (FR20)</p>	e.g., Los Bermejales Health Care Centre. Alemania St. Seville, 41018. Spain

 Requirement Consolidation II Appendix A	Document Short name: D5.2.3	
	Version:	1.0
D5.2.3	Date:	31/01/2013

Name of the Facility		Max		For instance, the name of the building: Los Berrmejales
Street Address		Max		Alemania Street
City		Max		Seville
State or Province		Max		Seville
Zip or Postal Code		Max		41018
Telephone		Max		+34 954123123
Contact email of the centre or of the prescriber		Max		losbermejaleshealthcentre@xx.es
Country	The country where the prescription was made	MS	The dispenser needs to know the country where he is consulting the information from	Spain
Prescriber Organization:			This is not a field but a block of information made up of the following fields. This might not be in the dataset but this information needs to be available for the process traceability (FR20)	
Organization Name		Max		e.g. Andalusia Health Service
Organization Identifier		Max	This field can be numbers	123458xfs

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

			and/or letters	
--	--	--	----------------	--

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.8.1.2 e1-FLD-136 Computational Dimension

3.8.1.2.1 e1-REQ-4576 Additional services 112 process

Related to e1-REQ-3846 112 Additional Service State Diagram

Description

General overview of the medical emergency handling process can be divided into three steps. In the first one, the emergency call is received in 112 Emergency Call Centre, first data about the situation are taken and medical resources are dispatched. In the second step, health professionals arrive to an emergency place and take care of the patient. The next step is when the patient arrives to the first aid department. Service description also implements a new functionality – Health Care event feedback delivery to the Patients EHR system in his Country.

Primary actors

Patient

Caller

Secondary actors

112 call – taker

Health Professional in the 112 call centre

Health Professional in the ambulance (Point of Care)

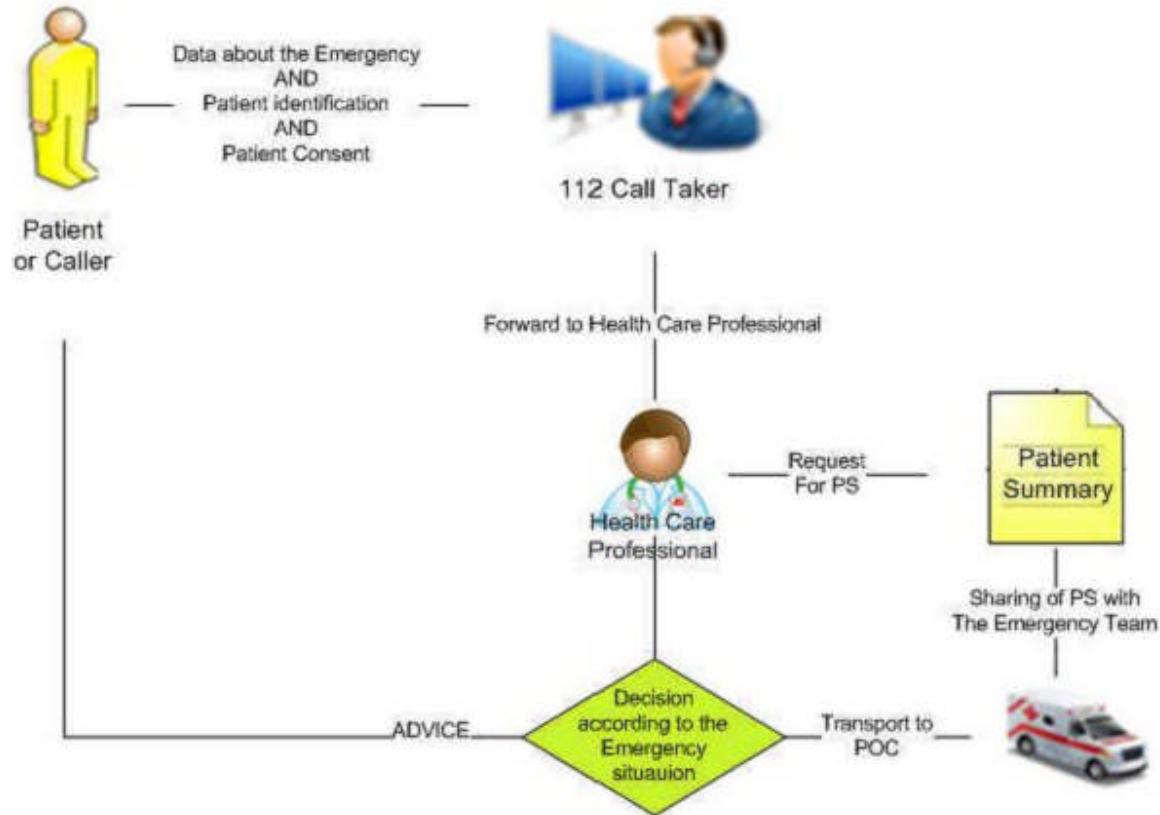
Health Professional in the first aid department (Point of Care)

Information used

The information used in the Use Cases for Additional services 112 is:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

The Patient Summary (PS)



	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.8.1.2.2 e1-REQ-3846 112 Additional Service State Diagram

Related to e1-REQ-2151 112 FR1 Integration of national infrastructure with 112 Emergency provider

Related to e1-REQ-2163 112 FR10 Inclusion of Emergency 112 identified physicians

Related to e1-REQ-2164 112 FR11 Authorized configuration of PS subset for 112 Emergency

Related to e1-REQ-2166 112 FR12 Supplement the data related to Emergency 112

Related to e1-REQ-2168 112 FR13 Definition of User interface

Related to e1-REQ-2170 112 FR14 Definition of Emergency User Interface

Related to e1-REQ-2171 112 FR15 Defining the proposition of the presented content for 112

Related to e1-REQ-2152 112 FR2 Integration of POC in the role of partner of 112 Emergency services

Related to e1-REQ-2153 112 FR3 Connectivity of 112 Emergency teams

Related to e1-REQ-2156 112 FR5 Identification of not communicating patient

Related to e1-REQ-2157 112 FR6 Patient consent and non-communicating patient

Related to e1-REQ-2159 112 FR7 PS data access logging

Related to e1-REQ-2160 112 FR8 Uniformity of implementation of the directives by PNs

Related to e1-REQ-2161 112 FR9 Selection and publication of data from epSOS patient summary to subset for 112 Emergency purpose

Related to e1-REQ-2173 112 NFR16 Availability of service

Related to e1-REQ-2175 112 NFR17 Availability of national PS repository

Related to e1-REQ-2176 112 NFR18 Availability of national 112 Emergency subset service

Related to e1-REQ-4576 Additional services 112 process

Related to e1-REQ-5094 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-5107 Data Integrity

Related to e1-REQ-5120 Data Origin and Data Authenticity

Related to e1-REQ-5103 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-5111 NFR05- Access control

Related to e1-REQ-5114 NFR09- Trust between countries

Related to e1-REQ-5079 Patient Identification

Related to e1-REQ-5083 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-5088 Willful Disclosure (Data Confidentiality)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Related to e1-REQ-5091 Willful Provisioning of Data (»Consent-1«)

Service pre-requisites:

Patient identification and authentication already exists

Health Professional identification and authentication already exist

National 112 Service provider already exists

National 112 Service provider is technically equipped to be connected to services enabling patient identification remotely

National 112 Service provider is technically equipped to receive patient consent remotely

POC is connected to NCP B and able to provide emergency event feedback to the NCPA (Patients EHR)

Country providing Health Care has functional NCP

The patient has filled PS in his NCP in the Country B

112 Emergency team member is a physician, who has access to the NCP (from legal and technical perspective).

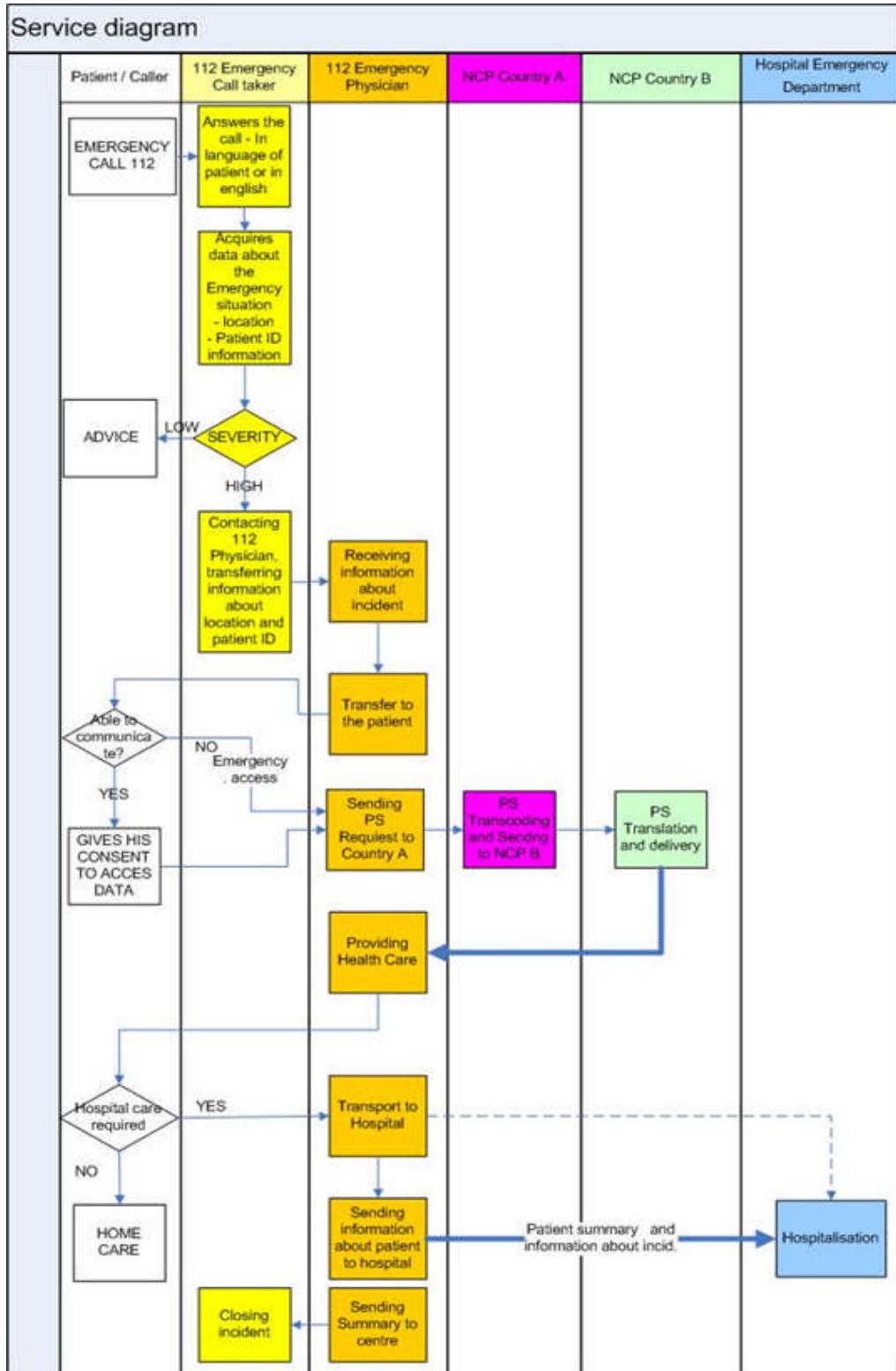
Existence of information channel between 112 emergency centre and 112 emergency team working in the field.

112 Call-taker understands the language of the patient or can communicate in English.

Legal compliance

Semantic interoperability

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013



	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.8.2 e1-FLD-87 Logical Perspective

3.8.2.1 e1-FLD-114 Service Functional requirements

3.8.2.1.1 e1-REQ-2151 112 FR1 Integration of national infrastructure with 112 Emergency provider

Related to e1-REQ-3846 112 Additional Service State Diagram

An initial agreement and interaction model between NCP national communication layer and belonging national infrastructure with the national 112 Emergency service provider should be established. This agreement should also address the presence of a physician having access rights for PS during, or immediately after emergency phone call.

3.8.2.1.2 e1-TXT-707 Note

Actors:National eHealth operator (epSOS beneficiary), Agencies responsible for local 112 Emergency services, 112 Emergency Physician, epSOS NCP

Preconditions:

Existence of 112 Emergency service organization in the Country

Local legislation (regulation) for information exchange exist

112 Emergency call answered or connected to physician

3.8.2.1.3 e1-REQ-2152 112 FR2 Integration of POC in the role of partner of 112 Emergency services

Related to e1-REQ-3846 112 Additional Service State Diagram

Integration of Emergency departments of hospitals (Emergency POC) interacting with the 112 Emergency service providers MUST be established as means to enable access to Patient summary immediately after patient arrival from emergency situation.

3.8.2.1.4 e1-TXT-708 Note

Actors: National eHealth operator (epSOS beneficiary), Agencies responsible for local 112 Emergency services

Preconditions:

Existence of 112 Emergency service organization in the Country

Local legislation (regulation) for information exchange exist

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.8.2.1.5 e1-REQ-2153 112 FR3 Connectivity of 112 Emergency teams

Related to e1-REQ-3846 112 Additional Service State Diagram

Technical infrastructure to enable communication (reception and transmission of data) to and from point of care MUST be available.

3.8.2.1.6 e1-TXT-709 Note

Associated Goals:

Transmission and reception of data in the field

Actors: Health Professional – Member of Emergency Team, Call Center operator (optional)

Preconditions:

National 112 Service provider is technically equipped to be connected to services enabling communication of epSOS related data remotely (ambulance, Emergency dept.)

3.8.2.2 e1-FLD-115 Service ID Management Requirements

3.8.2.2.1 e1-REQ-2156 112 FR5 Identification of not communicating patient

Related to e1-REQ-3846 112 Additional Service State Diagram

In situations where the patient cannot communicate a special approach for patient identification should be considered.

Services should be designed to eliminate errors, which could result in incorrect identification, as far as possible.

3.8.2.2.2 e1-TXT-711 Note

Identification of patient in the context of 112 Emergency technically runs in the same mode as in the case epSOS phase 1.

Associated Goals:

Improving Patient identification

Actors: Health Professional – Member of Emergency Team, Citizen from Country A, Call Center operator (optional)

Preconditions:

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

National 112 Service provider is technically equipped to be connected to services enabling patient identification remotely

3.8.2.2.3 e1-REQ-2157 112 FR6 Patient consent and non-communicating patient

Related to e1-REQ-3846 112 Additional Service State Diagram

Special approach for situations where the patient cannot communicate MUST be considered. That means a procedure, which allows the creation of the event recorded as inability to interact with the patient in obtaining his consent to access his PS must be established.

3.8.2.2.4 e1-TXT-712 Note

Associated Goals:

Improvement of existing process Logging of the data request

Actors: Health Professional – Member of Emergency Team, epSOS NCP, Call Center operator (optional)

Preconditions:

Patients EDS exists

HP connected to NCP

Identification data (ID present)

3.8.2.2.5 e1-REQ-5079 Patient Identification

Synchronized with e1-REQ-1973 Patient Identification

Related to e1-REQ-3846 112 Additional Service State Diagram

The intended recipient of medical data MUST identify the patient with sufficient accuracy. Medical data MUST only be disclosed after the patient was identified with sufficient accuracy.

Technical means for patient identification MUST NOT use or disclose medical data about this patient. Patient identifiers SHOULD NOT technically enable any unlawful linkage of the patient's medical data to other sanctioned personal data beyond any legitimate purpose from other domains. If technical means for identity protection (e.g. pseudonymization) are used, these MUST NOT disqualify the responsible parties to lawfully provide the patient access to his/her data. The original identification of the patient MUST NOT rely on the existence of electronic identifiers (eIDs). epSOS use cases MAY define further constraints on the accuracy and means of patient identification for that specific use case (e.g. identification by name considered as insufficient for the 112 use case).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.8.2.2.6 e1-TXT-710 Note

Associated Goals:

Improving identification across the PN

Actors: Health Professional–Member of Emergency Team, Citizen from Country A, Call Center operator (optional)

Preconditions:

Acceptance of identification mechanism by 112 Emergency provider

Electronic support is available in call centers and ambulances

Patient ID number or similar is requested in emergency call centers to identify the patient

3.8.2.3 e1-FLD-116 Service Legal requirements

3.8.2.3.1 e1-REQ-2159 112 FR7 PS data access logging

Related to e1-REQ-5083 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-3846 112 Additional Service State Diagram

Distributed Environment of Services 112 MUST be able to log the important events associated with the cross boarder patient data access.

Detailed information in the form of logs allowing a transparent way to get an overview, who, when and why accessed PS MUST be documented and available.

3.8.2.3.2 e1-TXT-713 Note

Associated Goals:

Legal reasons

Security reasons

Actors: Health Professional from country A, NCPs

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.8.2.3.3 e1-REQ-2160 112 FR8 Uniformity of implementation of the directives by PNs

Related to e1-REQ-3846 112 Additional Service State Diagram

The status and the uniformity of implementation of the relevant Directives in the member States and the participating non EU PNs MUST be verified.

3.8.2.3.4 e1-TXT-714 Note

Associated Goals:

Legal reasons

Security reasons

Actors: 112 Emergency services operators, National eHealth operators

The aspects of the organization of the actual services, from health systems legal perspective, has the same implications as that of the Patient summary.

3.8.2.3.5 e1-REQ-2161 112 FR9 Selection and publication of data from epSOS patient summary to subset for 112 Emergency purpose

Related to e1-REQ-3846 112 Additional Service State Diagram

Content selection of a retrieved epSOS Patient Summary according to legislative requirements of each participating nation MUST be facilitated.

3.8.2.3.6 e1-TXT-715 Note

Associated Goals:

Legal reasons

Security reasons

Actors: 112 Emergency services operators, National eHealth operators

Providers of services proposed in KT 1.4.8 (emergency teams acting in the field) need to have access to relevant Patient data which may have various form from country to country.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.8.2.3.7 e1-REQ-5083 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-3846 112 Additional Service State Diagram

Related to e1-REQ-2159 112 FR7 PS data access logging

Cross-border exchange of medical data MUST be documented in a fully traceable, reconstructable, and seamless fashion.

Cross-border exchange of medical data MUST produce a usable chain of digital evidence that enables both, the patient and his assigned DPA, to pursue, enforce, and proof any assumed or detected violation of the patient's data protection and privacy rights.

The chain of digital evidence MUST disclose the minimum of personal health data required to serve its purpose and MUST be specifically safeguarded against wrongdoing. Part of these safeguards MUST be a protocol that is not accessible to HPs.

Implications:

Audit trails SHOULD be written at both NCPs. For the purpose of data minimization NCP audit trails SHOULD not include medical data but just refer to (and safeguard) respective audit trails within HP systems.

3.8.2.3.8 e1-REQ-5088 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-1977 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-3846 112 Additional Service State Diagram

Medical data MUST NOT be disclosed to persons or organization unless they have been authorized by the patient (see »Consent-2; PIN«) and the disclosure is legally or explicitly required for fulfilling the treatment.

Medical data MUST NOT be disclosed to others than healthcare professionals or healthcare professional organizations in any case.

Medical data MUST NOT be transferred to other destinations unless this disclosure has been authorized by the patient or is mandated by national law.

The proper enforcement of the willful disclosure acc. to »consent-2« MUST be controllable and verifiable by the patient.

Implications:

Data MUST be encrypted during transfer and whenever it is stored at (intermediate) nodes outside the trusted environment of an HP (see "IT-Systems directly controlled by HPs").

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Depending on how “controllable” and “verifiable” are defined this requirement as well implies a need for secure end-to-end encryption between trusted HP environments.

3.8.2.3.9 e1-REQ-5091 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-1974 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-3846 112 Additional Service State Diagram

The provisioning of medical data for cross-border medical use cases MUST require a willful and documentable act of agreeing by the patient.

This willful act MUST fulfill all requirements of an informed, free consent acc. to country-A legislation. It MUST deliver an appropriate level of data security and privacy for the patient as it is defined in his home country.

This willful act MUST be designed in full anticipation of a cross-border health data exchange scenario.

The respective consent MUST be given in written form and MUST be signed by the patient. A qualified digital signature MAY be used instead of a wet signature.

A country MUST assure that patient data is only accessible if a valid patient consent for data provisioning exists. A country MUST ensure that data is no longer accessible after the respective consent has been revoked or expired.

A HP- B is not required to explicitly verify the existence of a patient's »consent-1« (that was formerly given in country-A) as it is assumed that all epSOS country-A have established secure processes for enforcing the revocation of consents and therefore will not provide data to a country-B unless a valid »consent-1« exists.

3.8.2.3.10 e1-REQ-5094 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-1975 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-3846 112 Additional Service State Diagram

Triggering a cross-country transfer of medical data MUST require a willful act by the patient.

This willful act MUST express the patient's explicit authorization to allow an identifiable healthcare professional the execution of defined data access operations.

This willful act MUST express the explicit authorization of the patient to transfer medical data to the formerly identified and specifically documented destination.

Countries MAY require that this willful act is documented by an explicit, written and informed consent that is to be signed by the patient.

Implications:

The authorization to perform a specific operation can only be given and documented in country-B (as this authorization requires the identification of both the patient and the HP-B).

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Therefore epSOS MUST provide technical means to transmit information about the authorization/PIN to country-A before or while a data access operation is triggered.

3.8.2.3.11 e1-TXT-845 Note

Associated Goals:

Manifesting the legal foundation for a lawful data processing

Granting the patient his specific rights according to data protection regulations

Deciding on whether a certain request for data is legitimated by the consent or not

Actors: Patient, Health professional

3.8.2.4 e1-FLD-117 Service Security requirements

3.8.2.4.1 e1-REQ-2163 112 FR10 Inclusion of Emergency 112 identified physicians

Related to e1-REQ-3846 112 Additional Service State Diagram

For physicians belonging to 112 emergency services identification mechanism and distribution of electronic certificates (the same as for epSOS + physicians in the hospital) MUST be ensured to allow access to the NCP.

3.8.2.4.2 e1-TXT-716 Note

Associated Goals:

Transparent access

Actors: NCPs, Health Professionals

3.8.2.4.3 e1-REQ-2164 112 FR11 Authorized configuration of PS subset for 112 Emergency

Related to e1-REQ-3846 112 Additional Service State Diagram

Configuration of the 112 emergency subset based on epSOS Patient summary MUST be carried out only by an authorized person through a specialized interface allowing each PN create and administrate its own national subset and its variants.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.8.2.4.4 e1-TXT-717 Note

Associated Goals:

Transparent access

Legal reasons

Actors: NCPs, Health Professionals

3.8.2.4.5 e1-REQ-5103 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-2206 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-3846 112 Additional Service State Diagram

epSOS agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations must be secured and codes of conduct as part of the epSOS Information Governance must be elaborated.

3.8.2.4.6 e1-REQ-5107 Data Integrity

Synchronized with e1-REQ-1978 Data Integrity

Related to e1-REQ-3846 112 Additional Service State Diagram

The integrity of transmitted data MUST be preserved when information is transmitted between different entities (legally or technically defined). It must be verifiable to a data receiver that data has not been damaged, altered or (partially) lost.

3.8.2.4.7 e1-REQ-5111 NFR05- Access control

Synchronized with e1-REQ-3880 NFR05- Access control

Related to e1-REQ-3846 112 Additional Service State Diagram

As authorisations involve the existence of a treatment context inside a HCPO, these treatment relationships must be justifiable on demand. The communication partners (origin, destination, and potential facilitators) MUST be known to each other with prior positive verification that all involved partners are authentic (security features to be provided by the means of an identity (subjects, actors, objects) and access management).

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.8.2.4.8 e1-TXT-855 Note

Associated Goals:

For traceability reasons

For security reasons

To assure confidentiality

For Confidentiality and integrity of medical data reasons

To align to the European Data Protection Regulations

3.8.2.4.9 e1-REQ-5120 Data Origin and Data Authenticity

Synchronized with e1-REQ-1984 Data Origin and Data Authenticity

Related to e1-REQ-3846 112 Additional Service State Diagram

The intended recipient of a medical data communication MUST be able to determine the originator and level of authenticity of the medical data received. Information on the identity and authenticity of the data originator that is assigned to the data or its metadata MUST NOT be altered during cross-border transfer.

3.8.2.4.10 e1-TXT-857 Note

Associated Goals:

To guarantee that the issuer of the information exchanged cannot refuse that the issuance has taken place

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.8.2.5 e1-FLD-118 Service Clinical requirements

3.8.2.5.1 e1-REQ-2166 112 FR12 Supplement the data related to Emergency 112

Related to e1-REQ-3846 112 Additional Service State Diagram

Emergency situation related data MUST be expressed in fashion of a clear comprehensible user interface based on present content of epSOS patient summary.

Through these user interface intervening physician MUST be able to receive data which may significantly affect the quality of health care provided in emergency situation.

Only allergies, current medical conditions and active prescriptions should be of most relevance for rendering with the User Interface.

3.8.2.5.2 e1-TXT-718 Note

Rationale:

During emergency transfer of a patient to an emergency facility, ambulance staff typically has an ample time and opportunity to be occupied with a patient's medical history or past medication.

Associated Goals:

Definition of User interface containing data relevant for
emergency situation

Actors: Clinical expert team, Emergency physician, Semantic expert team

3.8.2.6 e1-FLD-119 Service Semantic requirements

3.8.2.6.1 e1-REQ-2168 112 FR13 Definition of User interface

Related to e1-REQ-3846 112 Additional Service State Diagram

According to the opinion presented by many NEPCs and professional involved the design and specification of a specific User Interface for 112 Emergency purposes MUST be established.

Content of the User Interface for 112 Emergency purposes MUST be tailored to the needs of 112 Emergency teams.

The User interface SHOULD NOT include new concepts, just extract of relevant terms from existing epSOS patient summary.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Form and exact position of each data element MUST be fully configurable to fulfil all potential requirements of any Participating nation.

3.8.2.6.2 e1-TXT-719 Note

Actors: Semantic expert team, Clinical expert team, 112 Emergency physician

3.8.2.7 e1-FLD-120 Service Usability and data presentation requirement

3.8.2.7.1 e1-REQ-2170 112 FR14 Definition of Emergency User Interface

Related to e1-REQ-3846 112 Additional Service State Diagram

The Emergency User Interface MUST be designed in an understandable form.

The presentation layer must be designed to be as clear as possible.

Relevant information must be highlighted so that the 112 Emergency personnel is pointed to their seriousness.

3.8.2.7.2 e1-TXT-720 Note

Actors: 112 Emergency teams, Physicians providing Health Care

3.8.2.7.3 e1-REQ-2171 112 FR15 Defining the proposition of the presented content for 112

Related to e1-REQ-3846 112 Additional Service State Diagram

List of different data subsets from epSOS Patient summary, which reflect the needs of 112 emergency teams, should be stored as templates including the elements of interest and their position/layout on the screen used by different PN.

The following contents for such template for 112 Emergency purposes should be considered: patient's identification, actual and past medication, allergies, current medical condition, implants and other relevant information.

3.8.2.7.4 e1-TXT-721 Note

Actors: Semantic expert team, Clinical expert team, 112 Emergency physician

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.8.2.8 e1-FLD-121 Service Non-functional requirements: service level requirements

3.8.2.8.1 e1-REQ-2173 112 NFR16 Availability of service

Related to e1-REQ-3846 112 Additional Service State Diagram

At the level of operators, high availability of systems providing PS should be assured, given the nature of the Emergency services. Continuous service availability should be provided and the risk of technical failures should be minimized.

3.8.2.8.2 e1-TXT-722 Note

Actors: epSOS service provider

Preconditions Technical, infrastructure available high availability features.

3.8.2.8.3 e1-REQ-5114 NFR09- Trust between countries

Synchronized with e1-REQ-4564 NFR09- Trust between countries

Related to e1-REQ-3846 112 Additional Service State Diagram

All the countries involved in the project are integrated into one circle of trust (technical). An agreed framework for creating trust MUST be established, encompassing processes and procedures for critical data protection, privacy and confidentiality issues as well as mechanisms for their audit. Such issues include, but are not limited to:

- Identification, authentication and authorisation mechanisms
- Security and trust mechanisms
- Recording and exchanging patient consent

3.8.2.8.4 e1-TXT-858 Note

Associated Goals:

To enable the exchange of information between countries.

To avoid having to identify all professionals and institutions from a foreign country in the country of origin. On the one hand, each HP will be unequivocally identified and authenticated in his local system and must be identified based on his/her role/profile. On the other hand, Health Care Provider Organisation provides HP a status, a function, an authentication from which the HP trust is derived. Furthermore, Health Authorities Institutions assign and assure the status, the role, and sometimes the authentication of HP .

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.8.2.9 e1-FLD-122 Additional Architecture NCP / Central Service requirements

3.8.2.9.1 e1-REQ-2175 112 NFR17 Availability of national PS repository

Related to e1-REQ-3846 112 Additional Service State Diagram

PS repository containing patient's data MUST be available.

3.8.2.9.2 e1-TXT-723 Note

Actors: NCPs, Architects on national HIS

3.8.2.9.3 e1-REQ-2176 112 NFR18 Availability of national 112 Emergency subset service

Related to e1-REQ-3846 112 Additional Service State Diagram

Services generating subsets from Patient summary MUST be available. Subsets should be generated respecting national policy for content and data presentation.

3.8.2.9.4 e1-TXT-724 Note

Actors: NCPs, Architects on national HIS

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.9 e1-FLD-61 Patient Access Additional Service Specification

3.9.1 e1-FLD-88 Conceptual Perspective

3.9.1.1 e1-FLD-137 Computational Dimension

3.9.1.1.1 e1-REQ-4578 UC.PAC.1 Patient Access to PS or to eP in Country A with translation to Language B

Related to e1-REQ-3841 PAC Service State Diagram

Description

Cross-border distribution 1. Patient Access to Country A PS or eP, with translation to Language B, for own use:

Foreign language patients are by no means rare in any country. The potential for a widespread demand for the Use Case services is high, but the uptake may be rather slow.

Cross-border distribution 2. Patient Access to Country A PS or eP, for use in an encounter with a Health Professional in Country B:

The service process is the same as Use Case UC.PAC.1 in cross-border distribution 1, except for the final stage, where the Patient passes the epSOS document to his/her Health Professional -B. Also, the language of the epSOS translation may be dictated by the language of the New Health Professional, not necessarily that of the Patient. Therefore, this situation can also be seen as a workaround for the situation where the Country B Health Professional does not have access to the regular epSOS PS/eP documents – possibly even outside Europe. However, the Use Case still requires the semantic support for Language B, provided by an epSOS NCP.

Actors

The Patient

the HP in country B

the previous HP in country A,

the Patient Identification, Authentication and Authorization Service in Country A

the epSOS translation service

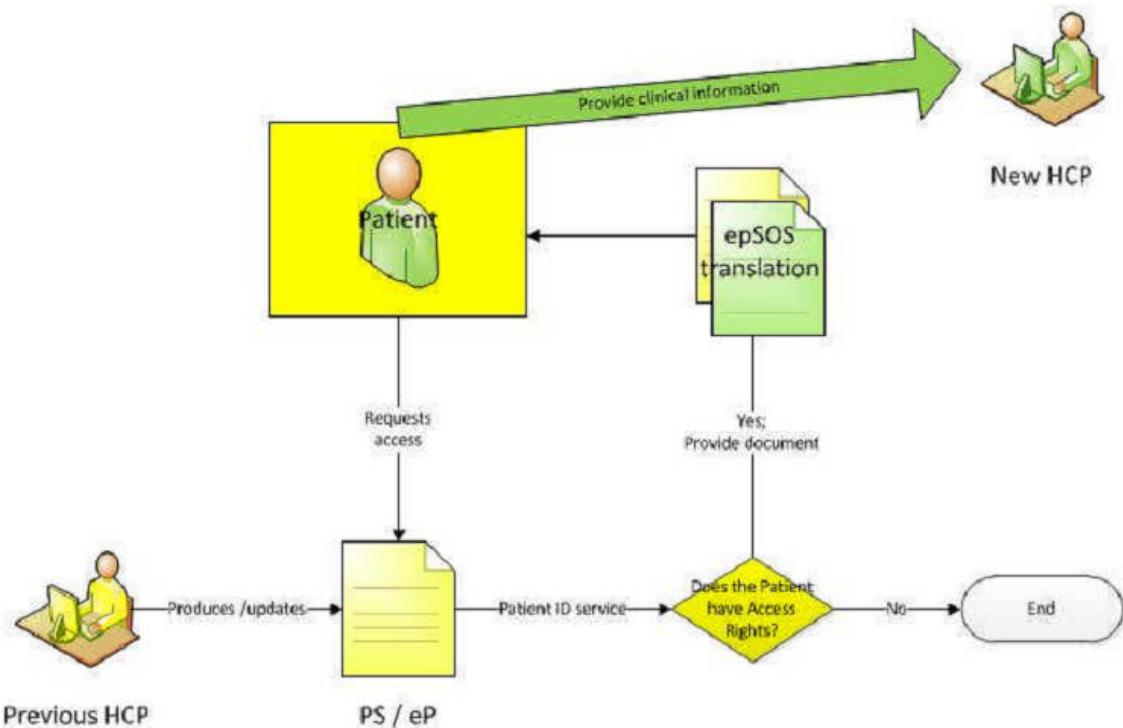
	Requirement Consolidation II Appendix A	Document Short name: D5.2.3 Version: 1.0
D5.2.3		Date: 31/01/2013

Preconditions

A Patient Summary or electronic Prescription exists in Country A

A National Patient Access Service exists in Country A

the epSOS translation service covers languages A and B



The Steps of the Use Case:

The Health Professional updates/produces the medical information used in the PS or eP on the basis of an encounter (i.e. the existence of a PS or eP is a precondition for the successful Patient Access Use Case)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

The Patient requests his or her PS or eP from the National Patient Access Service

The National Patient Access Service (including Patient Identification, authentication and role authorization) verifies that he or she has access rights to the information, including that his or her age is sufficient to allow access.

The National Patient Access Service provides the requested document

The epSOS Patient Access (PAC) service is invoked to produce a translation of (the coded content of) the document into Language B. The PAC service uses the MTC for Language B, produced by Country B.

The Patient receives the translated document.

The Patient reads, copies, uses and distributes the document as he or she considers appropriate.

One possible way the Patient may want to distribute the information to is a new Health Professional at a new encounter, scheduled or unscheduled. This step is relevant only if the Health Professional does not, for some reason, have access to the PS or eP.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.9.1.1.2 e1-REQ-3841 PAC Service State Diagram

Related to e1-REQ-5108 Data Integrity

Related to e1-REQ-5109 HCER-NFR02 Response time

Related to e1-REQ-5104 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-5122 NFR09- Trust between countries

Related to e1-REQ-2178 PAC FR01 Patient Access basic requirement

Related to e1-REQ-2179 PAC FR02 Patient identification and authentication: a univocal digital ID

Related to e1-REQ-2181 PAC FR04 Request from country A for a document translation

Related to e1-REQ-2182 PAC FR05 Delivered translation information is sent to country A

Related to e1-REQ-2183 PAC FR06 Information Traceability

Related to e1-REQ-2184 PAC FR07 Peering both original documents and translations

Related to e1-REQ-2187 PAC FR09 Data Translation Consistency

Related to e1-REQ-2188 PAC FR10 Clear responsibility assignment regarding the transformation of information by PAC functionalities

Related to e1-REQ-2189 PAC FR11 Unavailable information should remain unavailable to patients using PAC

Related to e1-REQ-2191 PAC FR12 Patient access to logs to his documents

Related to e1-REQ-2192 PAC FR13 Confidentiality of patient information

Related to e1-REQ-2195 PAC FR15 Labeling/Tagging of Chronicity character of diagnosis: Out of scope. Included for future developments

Related to e1-REQ-2197 PAC FR16 Semantic compliance

Related to e1-REQ-2198 PAC FR17 Disclaimer of scope of the translation service

Related to e1-REQ-2200 PAC FR21 PAC Service Availability

Related to e1-REQ-5080 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-4578 UC.PAC.1 Patient Access to PS or to eP in Country A with translation to Language B

Service pre-requisites:

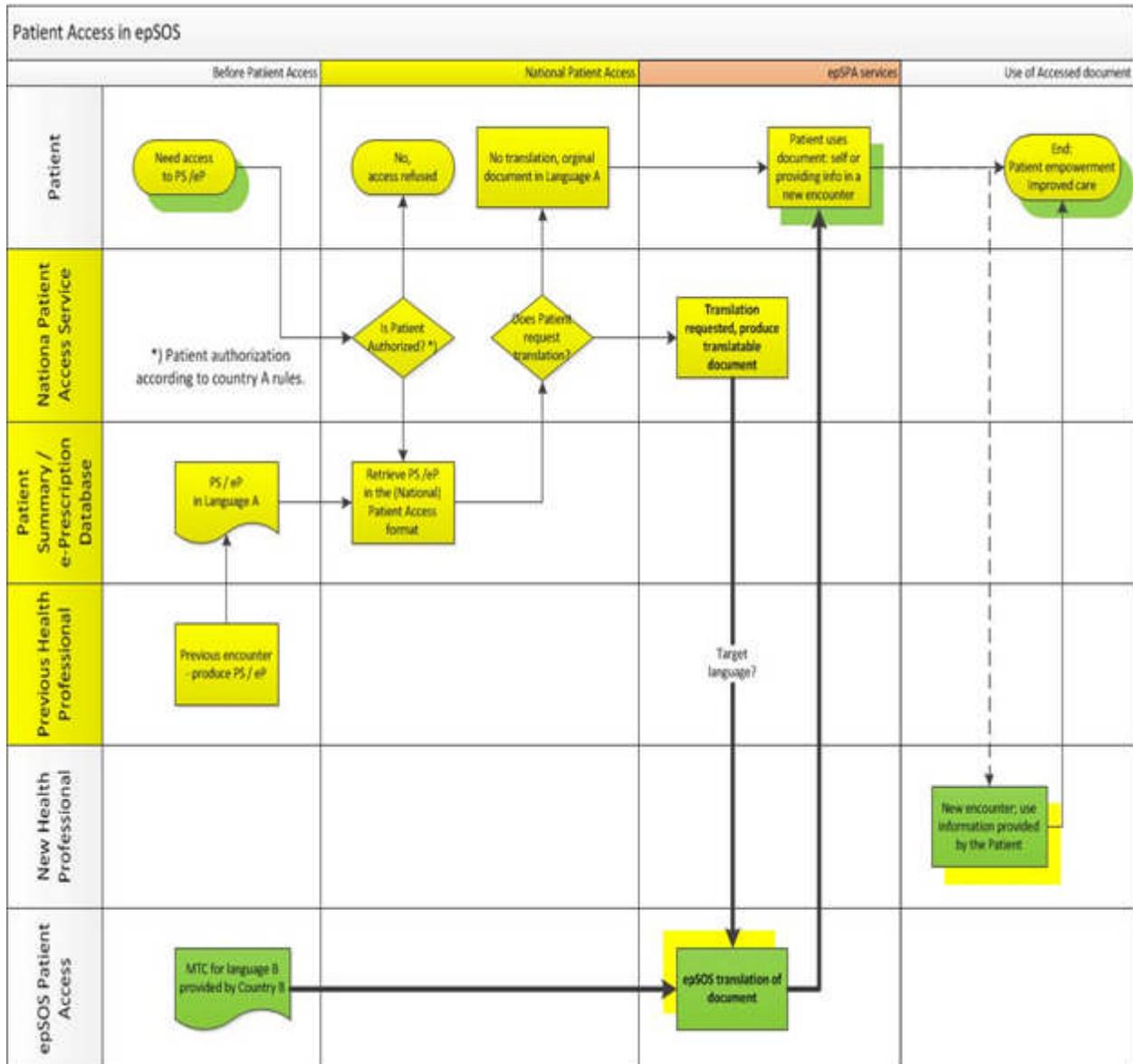
- Patient identification and authentication already exists
- Pre-existence of national EHR/PS and eP
- Transaction logging and transport security
- Country A is the only source of data for a patient.
- Neutrality: The functional specifications scenario does not make any assumptions on how

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

medical data is managed within a country A

- Scalability: The implementation should scale well with respect to the number of documents exchanged (or to the number of new value sets)
- Legal compliance: Original medical document ownership (owner is both the patient and the entity where the document is stored) and medical / legal validity of transformed document shall be analyzed according to the different PNs' laws.
- These functional specifications disclose use cases where country A has to somehow deal with medical data that is provided by a foreign physician.
- Semantic interoperability: epSOS Patient Access service (PAC) should guarantee the smoothest semantic transformation, keeping the meaning and the value of the original document, considering the liability for the transformation, and assuring the reproducibility of the semantic transformation.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013



Actions:

(This step is in the National Domain, and is a prerequisite for the PAC service)

- The patient affiliated in Country A requests access to PS or eP in Country A, by contacting the Country A National Patient Access Service

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

- The patient identifies himself
- The National Patient Access system verifies the patient's authorization
- The National Patient Access system retrieves the document

The Patient requests an epSOS translation of the retrieved document

The National Patient Access system passes the request to the epSOS NCP in Country A

The epSOS NCP in Country A provides a dialogue for selecting the source and target language (e.g. Language A, Language B; this should be provided based on the language list specified by the NEPC)

The National Patient Access system sends the document (in Language A) to the epSOS NCP in Country A

The NCP-A transforms (transcodes) the document indicated (or received) from Patient Access system into a translatable epSOS pivot document and then makes this pivot document available to the Translation Responsible.

The translation responsible retrieves the epSOS MTC of Language B

The translation responsible translates the pivot document and makes the translated document in language B available to NCP of country A

The NCP of country A conveys the information translated into the interface of the National Patient Access interface

The patient accesses the translated document in his specific device display

The use case is finished/closed

EXCEPTIONS:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The translation responsible does not have epSOS MTC of language B.

The translation responsible informs NCP of country A of the failure.

The NCP A cannot inform the Patient Access System / interface about the failure.

3.9.2 e1-FLD-89 Logical Perspective

3.9.2.1 e1-FLD-95 Basic Service Functional requirements

3.9.2.1.1 e1-REQ-2178 PAC FR01 Patient Access basic requirement

Related to e1-REQ-2211 L-HS-05 Manner and form of the right to access to health information by Patient

Related to e1-REQ-1972 Patient Access

Related to e1-REQ-3841 PAC Service State Diagram

The Patient must have the possibility to access his/her own medical information available at his/her national patient access (PAC) service (affiliation's country) and get it translated into any epSOS country language. Specific PAC services asks first its NCP-A for PS/eP translation service. As a consequence NCP-A should initiate a translation. Each translation request to an NCP-A must include these parameters:

Affiliation country where the Patient has identified/authenticated himself

Language of the Patient accessing the PAC Interface

Selected output language (translation language requested)

Language of document (the health information) accessed

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.9.2.1.2 e1-TXT-668 Note

Associated Goals:

Existing PS/eP in epSOS network must be available to patients either in his own language or in any of the languages of the participating PNs. After the identification of the patient who requests healthcare, in country A or B, the patient requests through a simple action (just a click) the visualization of the PS/eP in the selected language (that one that fits either with his own language or with that of the health professional).

The patient must be able to access his usual national Patient Access service.

National PA service asks NCP-A for the list of available translations service , and this list is sent and presented to specific Patient access service including for each access date/time of access.

Actors: Patient, Specific national patient access service, NCP A

Preconditions:

Pre-existence of national Patient access service

Pre-existence of epSOS NCPs, at both sides at the country having Patient access and in the output language requested by the patient.

3.9.2.1.3 e1-REQ-2179 PAC FR02 Patient identification and authentication: a univocal digital ID

Related to e1-REQ-3841 PAC Service State Diagram

epSOS Patient Access (PAC) must be in accordance with the Patient Access policy of patient's Country of Affiliation. Access by the patient to epSOS related functionalities through its National Patient Access shall not interfere with this rule. The patient MUST be univocally identified in a reliable way (unique and unequivocal id) to consult his information. Patient authentication MUST be guaranteed at national level based on the concept of mutual trust.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.9.2.1.4 e1-TXT-667 Note

Associated Goals:

To have certainty of the identity of the patient

Independence of national/regional PA systems. The responsibility for patient authentication and identification should remain within the patient's country of affiliation

Actors: Patient, National Certification authority in country A

Preconditions:

Pre-existence of digital certification authority. The certification authority has already assigned a digital ID to the patient.

There is a legal basis for access by citizens to their healthcare data in country A

Pre-existence of the Patient access service in country A

3.9.2.1.5 e1-REQ-2181 PAC FR04 Request from country A for a document translation

Related to e1-REQ-3841 PAC Service State Diagram

For any provided epSOS pivot content in structured form (both CDA level 1 and level 3), Country A MUST be able to request the translation of all coded elements that are used to describe the epSOS data set. Country A MUST provide original data in epSOS CDA compliant form, i.e. the friendly document that complies with the epSOS pivot document specifications.

3.9.2.1.6 e1-TXT-670 Note

Actors: NCP A, Translation's responsible (either Central services, NCP-A or NCP-B) to be decided at architectural level

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.9.2.1.7 e1-REQ-2182 PAC FR05 Delivered translation information is sent to country A

Related to e1-REQ-3841 PAC Service State Diagram

1. The translated information and metadata about the translation service must be sent to country A.
2. When creating a epSOS pivot document, in coded elements the information about code, code system and version should not be repeated in the translated element when the elements have the same values as in the original data.
3. The availability of the translation of the coded elements into the target language may depend on prior decisions taken by country B.
4. The information received by NCP-A must be delivered (must “talk”) to the specific National Patient Access service.
5. In the case that the PS or eP contain several items, this must be confirmed with the agreed CDA tool.
6. Country A NCP must answer/inform translation responsible of the successful receipt of the translation.

3.9.2.1.8 e1-TXT-672 Note

Associated Goals:

The NCP of country A must be informed about the delivered translation. Health care actions happening in country B as a result of Patient Access won't be reported back / won't be included! This is part of Use case PS extension.

Adaptation/integration/enlargement of current national Patient access services

Security reasons

Actors: Country A and B NCPs – depending on translation responsible, Common components in central services: CDA display tools

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.9.2.1.9 e1-REQ-2184 PAC FR07 Peering both original documents and translations

Related to e1-REQ-1988 Peering Original Document

Related to e1-REQ-3841 PAC Service State Diagram

Patient and healthcare professional must be able to consult a copy of the original document (with no epSOS semantic transformation) and the translated document.

3.9.2.1.10 e1-TXT-674 Note

Actors: Patient, Healthcare professional, NCP A,

Preconditions:

Availability of documents (eP/PS)

Availability of the pair of language translation involved

3.9.2.1.11 e1-REQ-2185 PAC FR08 Consultation of PoC through the patient access service-OPTIONAL

For the realm of epSOS the National Patient Access system may be able to retrieve the PoC through the NCP or from the epSOS website.

The patient may be able to identify from the result of available PoC the ones in the area where he is interested in for any type of health professional.

3.9.2.1.12 e1-TXT-675 Note

The patient triggers the event; the requested Point of Care in an area is the origin of the event; the Service consumer is NCP that triggered the event.

This may be a Browsing function returning the list of all PoC in the specified territory value set.

Associated goals:

Give guided access to epSOS web site maps/PoC.

Guided offer of a collection of retrieved PoC in www.epSOS.eu

Actors: Patient = Active participant, Directory/Value set of epSOS PoC www.epSOS.eu = Passive participant /object, Patient Access system calls NCP-A for this service

Preconditions:

Availability of PoC in the requested area (not mandatory). Return value may be zero

Correct PoC maintenance in www.epsos.euis under responsibility of the NABs

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.9.2.2 e1-FLD-94 Service Legal requirements

3.9.2.2.1 e1-REQ-2187 PAC FR09 Data Translation Consistency

Related to e1-REQ-3841 PAC Service State Diagram

The actual epSOS Circle-of-Trust (CoT) consists of pairs of mutually trusted consuming and providing gateways (NCPs). Countries allowing Patient access service to PS or eP SHOULD NOT update the previously given prior agreements. Translations delivered from the translation responsible to NCP A correspond up to 100% to those information stored and available in country A and this must be fully shown and MUST NOT be hidden to the patient.

3.9.2.2.2 e1-TXT-671 Note

Actors: National data storage systems, epSOS Framework Agreement

It is up to the national system were the data is stored and to ensure that EHR data not visible for the patient by means of national patient access service will also not be visible for the patient through utilisation of the epSOS Patient Access Service.

3.9.2.2.3 e1-REQ-2188 PAC FR10 Clear responsibility assignment regarding the transformation of information by PAC functionalities

Related to e1-REQ-3841 PAC Service State Diagram

Responsibility for each step of the transformation process from national EHR data or document into epSOS documents shall be clearly defined in epSOS phase 2 Liability Framework, and this information shall be made available to patients who wish to use PAC functionalities.

When the patient accesses epSOS related functionalities through his National Patient Access, country A patient MUST know that the translation may take place out of patient's country. Appropriate information for the patient covering the scope of available PAC functionalities must be accessible by the patient.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.9.2.2.4 e1-TXT-676 Note

Associated Goals:

Legal and liability reasons

Information to the patient

Protecting and safeguarding the patient's medical information

Actors: Country A, National EHR, NCP-A, NCP-B

PAC functionalities include the transformation of national EHR data or documents into epSOS documents, using transcoding and translation mechanisms based on MVC / MTC mechanisms. These epSOS transformed documents are then made available to the patient through the National Patient Access. This Functional Requirement controls the liability of the translation if the translation takes place out of patient's country.

3.9.2.2.5 e1-REQ-2189 PAC FR11 Unavailable information should remain unavailable to patients using PAC

Related to e1-REQ-3841 PAC Service State Diagram

Some national EHR system may implement "hiding" rules, which temporarily or not, hide specific information from patients.

The use of PAC functionalities by the patient should be compatible with the fulfillment of these rules.

3.9.2.2.6 e1-TXT-677 Note

Associated Goals:

Fulfillment of national rules concerning the level of availability of information

Actors: Country A, National EHR, NCP-A

Preconditions:

Rules of availability of information in country A

For example, information is stored within the patient EHR, but are not made available for access by the patient until a specific encounter takes place.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.9.2.2.7 e1-REQ-5080 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-1980 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-3841 PAC Service State Diagram

Cross-border exchange of medical data MUST be documented in a fully traceable, reconstructable, and seamless fashion.

Cross-border exchange of medical data MUST produce a usable chain of digital evidence that enables both, the patient and his assigned DPA, to pursue, enforce, and proof any assumed or detected violation of the patient's data protection and privacy rights.

The chain of digital evidence MUST disclose the minimum of personal health data required to serve its purpose and MUST be specifically safeguarded against wrongdoing. Part of these safeguards MUST be a protocol that is not accessible to HPs.

Implications:

Audit trails SHOULD be written at both NCPs. For the purpose of data minimization NCP audit trails SHOULD not include medical data but just refer to (and safeguard) respective audit trails within HP systems.

3.9.2.2.8 e1-REQ-2183 PAC FR06 Information Traceability

Related to e1-REQ-3841 PAC Service State Diagram

The information describing the process and the data involved in the process must be able to be retrieved. PAC functionalities include the transformation of national PS or eP into epSOS documents, using transcoding and translation mechanisms based on MVC / MTC mechanisms. These epSOS transformed documents are then made available to the patient through the National Patient Access. The information describing the process and the data involved in the transformation process must be traced and recoverable. It includes such information as the identification of the requester, steps in data transformation and timing of transformation. Main parameters for traceability of translation requested from an NCP-A to any translation responsible are:

Requester: Country of Patient identification/authentication

Country Language of the Patient accessing the PA Interface

Selected output language (translation language requested)

Language of the document (health information) accessed

Timing(time stamp) of the transformation

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.9.2.2.9 e1-TXT-673 Note

Associated Goals:

Security reasons

Legal and liability reasons

Actors: National Patient Access Service provider, National EHR subsystem, NCP-A, Translation responsible, NCP-B – depending on translation responsibility

3.9.2.3 e1-FLD-93 Service Security requirements

3.9.2.3.1 e1-REQ-2191 PAC FR12 Patient access to logs to his documents

Related to e1-REQ-3841 PAC Service State Diagram

Patients may be given possibilities to view all accesses done to his/her data, either by clinicians or by authorized persons.

3.9.2.3.2 e1-TXT-678 Note

This is linked to the “maintenance of patient consent” and to “patient access to access logs”. Some National Patient Access services are implementing similar components to let patients monitor who has accessed their EHR.

Associated Goals:

To provide a transparent means about the tenancy of the information

To give confidence to the patient through technical evidence about the correct access to patient's data

Actors: Central services

Preconditions & Post conditions:

Security audits of the NCPs (as in standard epSOS procedures)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.9.2.3.3 e1-REQ-2192 PAC FR13 Confidentiality of patient information

Related to e1-REQ-3841 PAC Service State Diagram

Whenever identifiable medical data is communicated, stored, or processed, the confidentiality of the data must be enforced and safeguarded by the epSOS LSP services (by all actors involved). All communication of identifiable data between the epSOS LSP partners must be performed in a way that prohibits any unwanted disclosure of medical data to any third party. Furthermore, the epSOS LSP services must enforce that any data access is only possible over safeguarded, well-defined interfaces.

An unwanted or unlawful disclosure to any unauthorized party must also be prohibited at all times.

3.9.2.3.4 e1-TXT-679 Note

Associated Goals:

Manifesting the legal foundation for a lawful data processing

Protecting and safe-guarding the patient's medical information

Actors: NCP-A, NCP-B, epSOS central services

3.9.2.3.5 e1-REQ-5104 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Synchronized with e1-REQ-2206 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-3841 PAC Service State Diagram

epSOS agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations must be secured and codes of conduct as part of the epSOS Information Governance must be elaborated.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

3.9.2.3.6 e1-REQ-5108 Data Integrity

Synchronized with e1-REQ-1978 Data Integrity

Related to e1-REQ-3841 PAC Service State Diagram

The integrity of transmitted data MUST be preserved when information is transmitted between different entities (legally or technically defined). It must be verifiable to a data receiver that data has not been damaged, altered or (partially) lost.

3.9.2.3.7 e1-TXT-680 Note

Associated Goals:

Trust in the system

Safety reasons

Detection of any damage or alteration to the data

Actors: NCP-A, Translation responsible, epSOS central services

3.9.2.4 e1-FLD-92 Service Clinical requirements

3.9.2.4.1 e1-REQ-2195 PAC FR15 Labeling/Tagging of Chronicity character of diagnosis: Out of scope. Included for future developments

Related to e1-REQ-3841 PAC Service State Diagram

Chronic diagnosis of a patient may be labeled in the PAC display tool what needs an enlargement of the value sets in PS.

“a chronic disease” label by which patients may be tagged would be very useful in future Use Case enlargement in epSOS for chronicity management.

This tagging may be done out of the combination of a specific set of diagnosis and specific active medication ATC codes together with date of prescription (begin-end or permanent condition of the medication)

Local terminology repositories may need to be synchronized for this issue.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.9.2.4.2 e1-TXT-681 Note

This will be discussed in KT 1.4.10.

Associated Goals:

To provide a list of epSOS chronic diseases with its corresponding ICD-9/ICD-10 codes under the wide consensus of epSOS

To ensure that the doctor/prescriber is familiar with the nomenclature

Actors: Central services, Local Terminology Repositories

Preconditions & Post conditions:

The EHR/PS or eP preexists in country A

MVC is enlarged with this new Data set and Value sets

In the future some “optional” data sets should become “mandatory” (=those relevant for chronicity)

3.9.2.5 e1-FLD-91 Service Semantic requirements

3.9.2.5.1 e1-REQ-2197 PAC FR16 Semantic compliance

Related to e1-REQ-3841 PAC Service State Diagram

Target language selection menu will be expressed at the user interface level in a familiar and well known way at every national Patient access system, but at PAC level, internally this should be kept in a form compliant with the epSOS specification (e.g. currently as a combination of ISO 639-1 (language tags) and ISO 3166-1 codes(country abbreviations).

Exchanged documents (both sent and received) must be compliant with the level 1 or 3 epSOS CDA R2 specifications (currently defined by the D3.9.1 Appendix B1 and B2 epSOS Semantic Implementation Guidelines]

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

3.9.2.5.2 e1-TXT-682 Note

Actors: Local Terminology Repositories, MVC

Preconditions & Post conditions:

Enlargement of the current Data sets

3.9.2.5.3 e1-REQ-2198 PAC FR17 Disclaimer of scope of the translation service

Related to e1-REQ-3841 PAC Service State Diagram

The patient shall be informed about the limitations of the translation. This requirement demands the PAC service explains to the patient the possible translation limitations, as part of the translation request dialogue, and also along with the translated document, informing that the service only translates the coded content of the PS/eP.

The original document accessible by Country A National Patient Access may include clinical information the PAC cannot translate, and the information not translated may have clinical relevance that the translated information does not cover.

3.9.2.5.4 e1-TXT-683 Note

Actors: Patient access service

Preconditions & Post conditions:

All exceptions occurred during transcoding or translation has to be reported to Workflow Manager using response structure

3.9.2.6 e1-FLD-90 Service Non-functional requirements

3.9.2.6.1 e1-REQ-2200 PAC FR21 PAC Service Availability

Related to e1-REQ-3841 PAC Service State Diagram

If possible, planned unavailability should take place during night hours and patients should be informed in advance.

Unplanned unavailability should be detected and corrected or circumvented as soon as possible.

In case of unplanned unavailability, procedures should be defined to allow for regular information of stakeholders and return to normal as soon as possible.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

3.9.2.6.2 e1-TXT-684 Note

The availability of PAC functionalities lies within the availability of different services (availability of national patient access, availability of transcoding processes, availability of translation processes, etc.). Each service may be unavailable for different reasons, planned or unplanned.

Associated Goals:

Continuous availability of PAC functionalities (> 99,5%)

Monitoring of service availability

Actors: National EHR, NCP-A, NCP-B, epSOS central services

3.9.2.6.3 e1-REQ-5109 HCER-NFR02 Response time

Synchronized with e1-REQ-2121 HCER-NFR02 Response time

Related to e1-REQ-3841 PAC Service State Diagram

The system SHOULD provide an average end to end response time within 5 seconds.
The average end to end response time MUST NOT be more than 10 seconds.

3.9.2.6.4 e1-TXT-852 Note

Associated goals:

The overall response time of PAC functionalities will depend on the response time of several different services.

The purpose is to deliver to the patient a global service with an acceptable response time.

3.9.2.6.5 e1-REQ-5122 NFR09- Trust between countries

Synchronized with e1-REQ-4564 NFR09- Trust between countries

Related to e1-REQ-3841 PAC Service State Diagram

All the countries involved in the project are integrated into one circle of trust (technical). An agreed framework for creating trust MUST be established, encompassing processes and procedures for critical data protection, privacy and confidentiality issues as well as mechanisms for their audit. Such issues include, but are not limited to:

- Identification, authentication and authorisation mechanisms
- Security and trust mechanisms
- Recording and exchanging patient consent

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

3.9.2.6.6 e1-TXT-863 Note

Associated Goals:

To enable the exchange of information between countries.

To avoid having to identify all professionals and institutions from a foreign country in the country of origin. On the one hand, each HP will be unequivocally identified and authenticated in his local system and must be identified based on his/her role/profile. On the other hand, Health Care Provider Organisation provides HP a status, a function, an authentication from which the HP trust is derived. Furthermore, Health Authorities Institutions assign and assure the status, the role, and sometimes the authentication of HP .

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4 e1-FLD-250 Testing

4.1 e1-FLD-251 Conceptual Perspective

4.1.1 e1-REQ-5217 Main participation rules for test phases

Related to e1-REQ-5216 Interactions among the epSOS test phases

Related to e1-REQ-5219 Conformance Gate 0 (CG0)

Related to e1-REQ-5220 Conformance Gate 1 (CG1)

Related to e1-REQ-5221 Conformance Gate 2 (CG2)

According to epSOS Testing Strategy, the **main participation rules** for the test phases pre-PAT, PAT and PPT are as follows:

A participant (PN or vendor) who has never achieved a PAT previously MUST start from pre-PAT and PAT.

This rule has an exception. Due to time constraints, if a new PN who has never achieved a PAT before shows very good progress with implementation and testing, then it MAY be allowed to start from PPT and PPT-slot instead of PAT. This exception can only be applied if the next PAT is several months ahead. This decision is evaluated individually for each requestor, and MUST be approved by KT3.C.4 leader, WP3.C leader, PD4 leader, the TPML and the PC. Even if this exception is approved, the corresponding PN MUST still participate to the next possible PAT.

If a participant is not able to achieve any progress during pre-PAT, then it is asked to de-register from the upcoming PAT.

The participants that achieved a PAT MUST proceed with PPT.

If the PNs who already achieved a PAT i) improve an existing service, ii) implement a new service, or iii) switch their NCP completely (e.g. from NCP-in-a-box to OpenNCP), then they are permitted to proceed with PPT and PPT-slot. It is NOT REQUIRED to start from PAT again.

The PNs MUST operate their PPT environments and participate in PPT activities starting from the end of a successful PAT and continuing as long as they remain in the epSOS network.

In order to proceed to pilot operation, a PN MUST achieve at least one PPT-slot. A PN who failed for a PPT-slot MUST participate to a new PPT-slot, if it is willing to be part of operation.

The PNs MUST NOT shut down their PPT environments and stop PPT activities after being accepted in operation.

A participant MAY participate to PATs and PPT-slots as many times as they want, even after becoming successful.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

It should be noted that these are only the main rules. The details of the participation criteria by means of conformance gates must be considered.

4.1.2 e1-REQ-5216 Interactions among the epSOS test phases

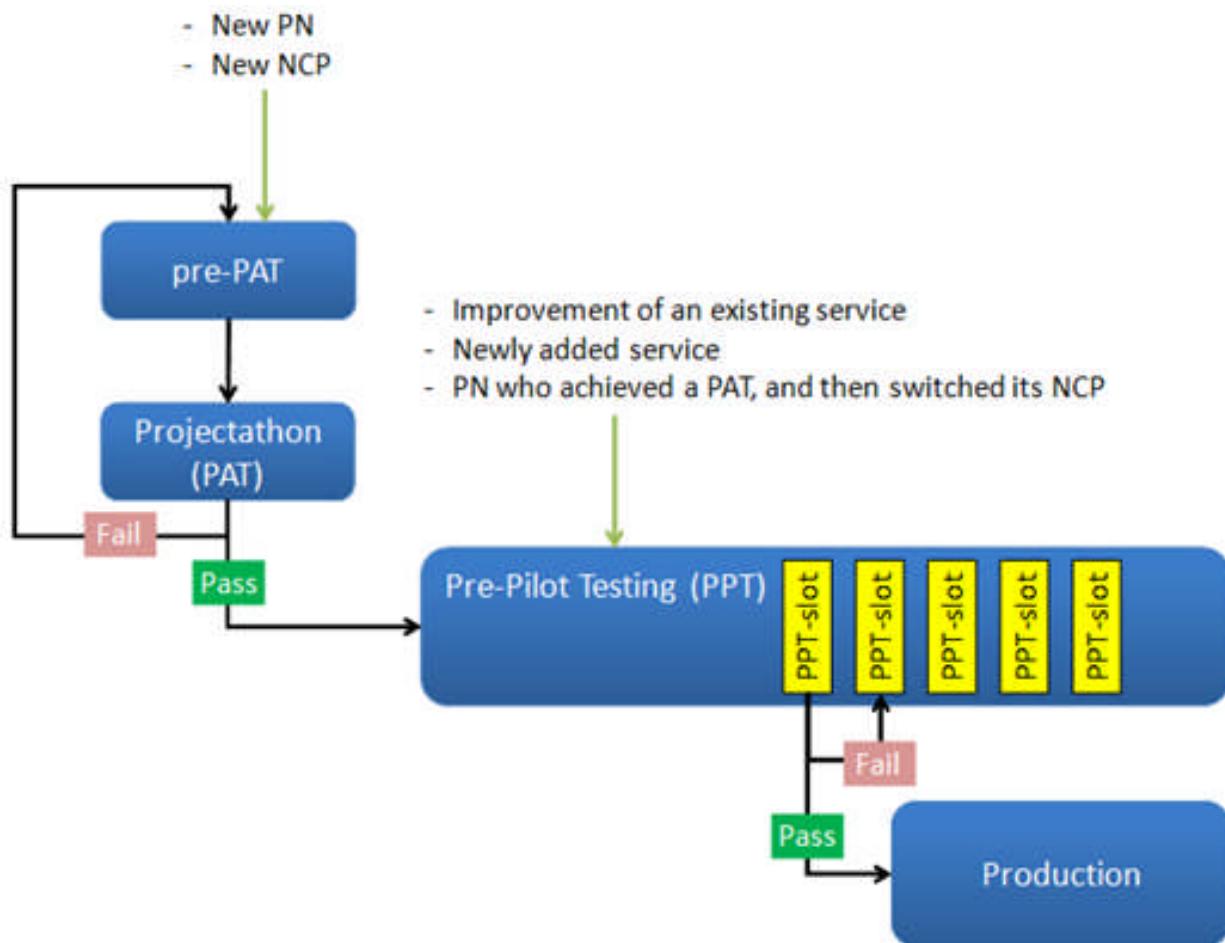
Related to e1-REQ-5207 Conformance Test (Pre-Projectathon)

Related to e1-REQ-5217 Main participation rules for test phases

Related to e1-REQ-5209 Pre-Pilot Test

Related to e1-REQ-5208 Service Interoperability Test (Projectathon)

The interactions among the epSOS test phases are depicted in the following figure.



	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.1.3 e1-FLD-262 Test Phases

4.1.3.1 e1-TXT-867 Note

Test phases are a distinct set of test activities collected into a manageable group. The term "phase" may suggest a strict chronological order. However, this is only partly correct, in principle:

Component level tests precede the System and Integration level tests.

The Component Test Phases precede the Service Test Phases which themselves precede the pre-Pilot test.

However, tests in a following phase can be conducted so long as the entry criteria for this phase have been met and where applicable dependent tests have been conducted. This requires that a Test Concept defines the Test Phases with their own entry and exit criteria superseding that of this Test Strategy. While this has the advantage of speeding up the test it requires additional effort and analysis in defining the Test Concepts.

This test strategy supports the following Test Phases:

Component Unit Test (CUT)

Component System Test (CST)

Component Integration Test (CIT)

Conformance Test (CCT) (Pre-Projectathon)

Service Interoperability Test (SIT) (Projectathon)

Pre-Pilot Test (PPT)

The following figure shows the relationship between the test levels and phases:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Positioning test levels and phases

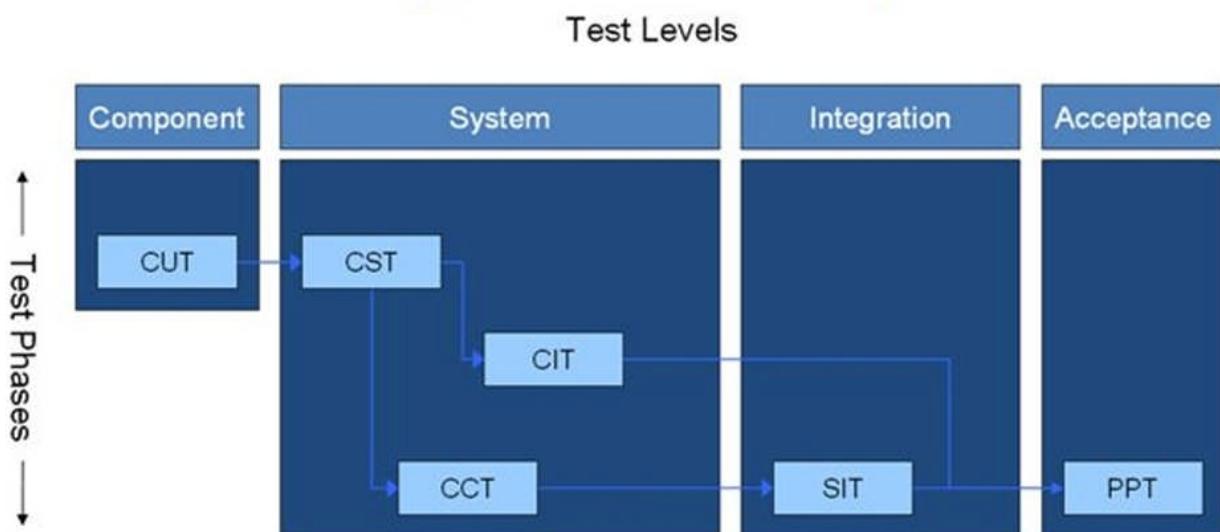


Figure - Levels and Phase

It should be noted that, testing by the PNs shall not be limited to these test phases. In addition to Component Unit Test (CUT), Component System Test (CST) and Component Integration Test (CIT) phases that are advised to the PNs, they are encouraged to use the simulators and validation services of IHE-Europe even during their development process. These simulators and validators are used normally during pre-PAT and PPT, but they are in fact available online almost 7/24.

4.1.3.2 e1-REQ-5204 Component Unit Test

Purpose

The Component Unit Test is the phase foreseen to test the software components (SWC). Its objective is to expose defects in the internal behaviour of the software component under test. The components are treated as white boxes and as such should be tested using appropriate white box techniques.

During this phase the components that make up the NCP, Portal and any other external service developed by epSOS or its subcontractors are tested. The goal is a fully tested component that is ready for the integration into a complete system.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Responsibility

Task / Organisation	epSOS / IHE-Europe	Participating Nation (Own development)	F.E.T. (NCP-in-a-T-box)	Industry (Components)
Test Planning		X	X	X
Test Design		X	X	X
Test Implementation		X	X	X
Test Execution		X	X	X
Test Evaluation		X	X	X

epSOS and F.E.T.

Where epSOS undertakes the development of a component, the accountability falls ultimately under epSOS but the responsibility for its execution can be assumed by epSOS or its sub-contractors / beneficiaries.

In the case of the NCP-in-a-Transparent-box, the responsibility falls under F.E.T.

In case of OpenNCP, the responsibility falls under the related OpenNCP mini-project team.

Where possible, epSOS[1] will provide Participating Nations with Test Stubs, Drivers, Simulators and Validators to support the testing of the epSOS trust domain interface. See D3.C.1 Appendix B # 6.2 for a list of available simulators and validators.

Participating Nations and Industry

The Participating Nations and the Industry are responsible for their component unit testing. This Test Strategy places no constraints or requirements on their test process.

Entry Criteria

The organisation tasked with the development of the component is to define its entry criteria. Due to the informality of this test phase epSOS places no constraints on its definition.

Exit Criteria

The following must be met and formally documented in order for the component to enter into the next test phase:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Requirement to modules coverage matrix showing implementation of all requirements with a priority of high and medium.

Internal testing coverage of all paths, branches, and conditions showing coverage:

For epSOS LSP	Code Coverage	Use of code-metrics / bug detection software
Gateway / high-priority SW	>80%	Yes / Yes
Support tools	>60%	Yes / Yes
GUI	-	No / Yes

No open problems of severity 1 and 2 as defined in D3.C.1 Appendix B # 3.6.3.1 Defect Classification.

No open problems of severity 3 as defined in this document without a functioning workaround.

Component under Configuration Management, versioned and base lined.

Workarounds are documented in the release notes.

When the defined exit criteria have not been met the Test Report must list the deviations and their estimated risk. In this case epSOS must decide if the component can take part in the next test phase.

Deliverables

The following are the expected deliverables:

A Test Report whose content is defined by the organisation conducting the tests, incorporating the results of the test; including as a minimum the information listed in the exit criteria; as verification that the tests have been completed.

[1] F.E.T. will not provide any simulators.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.1.3.3 e1-REQ-5205 Component System Test

Purpose

The Component System Test is the phase foreseen to functionally and non-functionally system test a software component. Its objective is to expose defects in the functional and non-functional behaviour of the software system under test. The systems are treated as black boxes and as such should be tested using appropriate black box techniques.

During this phase the system (NCP, Portal, or external services developed by epSOS) that is made up of the components tested during the component unit test phase will be tested. The goal is a fully tested system that is ready for integration testing.

Responsibility

Task / Organisation	epSOS / IHE-Europe	Participating Nation (Own development)	F.E.T. (NCP-in-a-T-box)	Industry (Components)
Test Planning		X	X	X
Test Design		X	X	X
Test Implementation		X	X	X
Test Execution		X	X	X
Test Evaluation		X	X	X

epSOS and F.E.T.

Where epSOS undertakes the development of a system, the accountability falls ultimately under epSOS but the responsibility for its execution can be assumed by epSOS or its subcontractors. In the case of the NCP-in-a-Transparent-Box, the responsibility falls under F.E.T.

In case of OpenNCP, the responsibility falls under the related OpenNCP mini-project team(s). In case the system is updated with PN-specific components by the adapting PNs, then it is also the PNs' responsibility to do Component System Tests.

Where applicable, epSOS will provide Participating Nations with Test Stubs, Drivers, Simulators and Validators to support the testing of the epSOS trust domain interface. See D3.C.1 Appendix B # 6.2 for a list of available simulators and validators.

Participating Nations and Industry

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

The Participating Nations and the Industry are responsible for their component system testing. This strategy places no constraints or requirements on their test process.

Entry Criteria

The following defines the entry criteria for admission to the Component System Test phase:

The exit criteria for the Component Unit Test phase have been met.

Availability of all component documentation including but not restricted to release notes, installation and configuration handbook, and user guide.

Availability of Workarounds

Exit Criteria

The following must be met and formally documented in order for the component to enter into the next test phase:

Requirement to test case coverage matrix showing 100% coverage of all functional, non-functional and non integrative testing requirements.

All Test Cases with a priority of 1 or 2 as defined in D3.C.1 Appendix B # 3.6.2.1 Test Case Priority, have the test result Pass.

70% of all test cases with a priority of 3 have been executed

All problems of severity 1 and 2 as defined in D3.C.1 Appendix B # 3.6.3.1 Defect Classification, are closed

All open problems of severity 3 have a functioning workaround and are described in the Test Report.

All Test Artefacts are under Configuration Management and Base lined.

System under Configuration Management, versioned and base lined.

System is available as an installable package (MSI, TAR, etc.)

When the defined exit criteria have not been met, the Test Report must list the deviations and their estimated risk. In this case epSOS must decide if the system can take part in the next test phase.

Deliverables

The following are the expected deliverables:

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

A Test Report, managed by the organization doing the tests, incorporating the results of the test; including as a minimum the information listed in the exit criteria; as verification that the tests have been completed.

The system must be provided in the form of an installable CD or downloadable package (MSI, TAR, etc).

4.1.3.4 e1-REQ-5206 Component Integration Test

Purpose

The Component Integration Test is the phase foreseen to test the interaction between two systems, which have previously been system tested. Its objective is to expose defects in the interfaces and the interaction with other previously tested systems and to verify that they are interoperable with one another.

This phase can only take place when a software producer develops a system that is required to be integrated with another system (actual or reference).

In the case that a software provider only develops a single system, they will have to wait until the Service Interoperability Test phase (Projectathon) before being able to integration test their systems with those developed by other software producers.

Responsibility

Task / Organisation	epSOS / IHE-Europe	Participating Nation (Own development)	F.E.T. (NCP-in-a-T-box)	Industry (Components)
Test Planning		X	X	X
Test Design		X	X	X
Test Implementation		X	X	X
Test Execution		X	X	X
Test Evaluation		X	X	X

epSOS and F.E.T.

Where epSOS undertakes the development of a system, the accountability falls ultimately under epSOS but the responsibility for its execution can be assumed by epSOS or its subcontractors. In the case of the NCP-in-a-Transparent-Box, the responsibility falls under F.E.T.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

In case of OpenNCP, the responsibility falls under the related OpenNCP mini-project team(s). In case the system is updated with PN-specific components by the adapting PNs, then it is also the PNs responsibility to do Component Integration Tests.

Where applicable, epSOS will provide Test Stubs, Drivers, Simulators and Validators to support the integrative testing of the epSOS trust domain interface. See D3.C.1 Appendix B # 6.2 for a list of available simulators and validators.

Participating Nations and Industry

The Participating Nations and the Industry are responsible for their component integration testing. This Test Strategy places no constraints or requirements on their test process.

Entry Criteria

The following defines the entry criteria for admission to the Component Integration Test phase:

The exit criteria for the Component System Test phase have been met.

Availability of updated component documentation including but not restricted to release notes, installation and configuration handbook, and user guide.

Availability of workarounds.

Exit Criteria

The following must be met and formally documented in order for the component to enter into the next test phase:

Requirement to test case coverage matrix showing 100% coverage of all integrative testing requirements.

All Test Cases with a priority of 1 or 2 as defined in D3.C.1 Appendix B # 3.6.2.1 have the test result Pass.

70% of all test cases with a priority of 3 have been executed

All problems of severity 1 and 2 as defined in D3.C.1 Appendix B # 3.6.3.1 Defect Classification are closed

All open problems of severity 3 have a functioning workaround and are described in the Test Report.

All Test Artefacts are under Configuration Management and Base lined.

Component base lined.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

When the defined exit criteria have not been met the Test Report must list the deviations and their estimated risk. In this case epSOS must decide if the system can take part in the next test phase.

Deliverables

The following are the expected deliverables:

A Test Report, managed by the organization doing the tests, incorporating the results of the test; including as a minimum the information listed in the exit criteria; as verification that the tests have been completed.

System is available as an installable package (installable CD, MSI, TAR, etc.).

4.1.3.5 e1-REQ-5207 Conformance Test (Pre-Projectathon)

Related to e1-REQ-5216 Interactions among the epSOS test phases

Related to e1-REQ-5219 Conformance Gate 0 (CG0)

Related to e1-REQ-5209 Pre-Pilot Test

Related to e1-REQ-5210 Pre-Projectathon and PPT-slot Test Cases (Conformance Tests)

Related to e1-REQ-5208 Service Interoperability Test (Projectathon)

Purpose

The Conformance Test is the phase foreseen to test the component or system against the pre-defined epSOS test cases as the pre-requisite for entry into the Service Interoperability Test (Projectathon). Its goal is to verify that all pre-defined test cases pass when executed against the component or system under test. It is also known as Pre-Projectathon Test (pre-PAT).

Conformance Testing is also done within the Projectathon and the PPT-slot.

Pre-Projectathon (pre-PAT) is the online (i.e. remote) conformance testing activity that is held prior to a Projectathon. The focus is on checking the compliance of the PN and vendor implemented systems to the epSOS Interoperability Profiles, messages and documents individually. For this purpose, the systems are tested against simulators and validators provided by the epSOS Project in cooperation with IHE-Europe. Completing the Pre-Projectathon is necessary for being allowed to go to the proceeding Projectathon.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Responsibility

Task / Organisation	epSOS / IHE-Europe	Participating Nation (Own development)	F.E.T. (NCP-in-a-T-Box)	Industry (Components)
Test Planning	X	X	X	X
Test Design	X			
Test Implementation	X	X	X	X
Test Execution		X	X	X
Test Evaluation	X			

epSOS, IHE-Europe and F.E.T.

Where epSOS undertakes the development of a system, the accountability falls ultimately under epSOS but the responsibility for its execution can be assumed by epSOS or its sub-contractors / Beneficiaries.

In the case of the NCP-in-a-Transparent-Box, the responsibility falls under F.E.T.

In case of OpenNCP, this time the responsibility falls under the adapting PNs and vendors, as OpenNCP itself is not a complete reference implementation, but a set of integrated components that have to be further completed by the adapting PNs / vendors.

As certain decisions pertaining to the division of work have already been taken these are reflected here.

Test Design is assumed by the beneficiary IHE-Europe and epSOS.

Test Implementation is assumed by the beneficiary IHE-Europe.

Test evaluation is assumed by the beneficiary IHE-Europe (third party).

Where applicable, epSOS will provide Participating Nations all necessary Test Stubs, Drivers, Simulators and Validators to support the conformance testing. See # 6.2 for a list of available simulators and validators.

A pre-PAT slot is announced prior to a Projectathon (PAT) by epSOS testing team and IHE-Europe, and is kept open for several weeks until the PAT itself. In the last 2-3 weeks before PAT, IHE-Europe validates the tests that are completed by the PNs / vendors against the conformance validators and simulators.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Participating Nations and Industry

Test Planning will be assumed by Participating Nations, F.E.T. or the Industry.

It is not ruled out that the Participating Nations, F.E.T. or the Industry have anything to implement.

Test Execution will be assumed by the Participating Nations, F.E.T. or the Industry.

Entry Criteria

Only the PNs and vendors that are registered for a Projectathon are allowed (actually, "have to") complete the corresponding Conformance Test session (i.e. pre-Projectathon Test). The registration is again managed by IHE-Europe and epSOS through the Gazelle tool.

The other conformance testing activities within the Projectathon and PPT-slot are part of the corresponding testing sessions.

Exit Criteria

As the entry into the Service Interoperability Test (SIT) (Projectathon) is dependent on the results of the Conformance Test, and the responsibility for SIT lies within epSOS, the following exit criterion applies to all software producers' epSOS, PN, vendors and software producers alike:

All Test Cases registered in Gazelle according to the implemented profiles are executed and have the test result Pass.

Deliverables

All who are to participate in the Service Interoperability Test (Projectathon) are to provide epSOS with their Conformance Test (pre-Projectathon) Results. The participants register their test logs through the Gazelle Management Tool as in the case of PAT, and the results are validated by IHE-Europe.

Following the audit of test results by IHE-Europe, epSOS provides the submitter with a confirmation of participation to proceed with the proceeding Projectathon.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.1.3.6 e1-REQ-5208 Service Interoperability Test (Projectathon)

Related to e1-REQ-5207 Conformance Test (Pre-Projectathon)

Related to e1-REQ-5216 Interactions among the epSOS test phases

Related to e1-REQ-5219 Conformance Gate 0 (CG0)

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Related to e1-REQ-5212 Test Cases for end-to-end Functional Testing

Purpose

The Service Interoperability Test is the phase to test the pre-defined test cases as defined by epSOS. The SIT has a Workshop characteristic and is conducted in a pre-determined location, within a pre-defined duration in which the test cases are executed. Participants register their interest and providing they meet the entry criteria can take part.

Its objective is to verify that all pre-defined functional, non-functional and integrative test cases pass when executed by:

A standalone component or system

A component that is integrated with other standalone components or systems

The goal is to verify the interaction of integrated components during the execution of end to end business processes.

The Service Interoperability Test is also known as Projectathon within the scope of epSOS. Projectathon is an interoperability testing event similar to Connectathon, organised and managed by the epSOS Project in cooperation with IHE-Europe, to assure the interoperability of the PN and vendor implemented systems according to the epSOS Interoperability Profiles. It is usually held together with European Connectathons. In addition to (some) conformance and (mostly) interoperability testing, Projectathon includes end-to-end functional testing with the involvement of HPs. PNs need not to participate with their actual national infrastructures to a Projectathon; a simulation of the national environment is accepted as well. Only the PNs who successfully pass a Projectathon are allowed to go to Pre-Pilot Testing.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Responsibility

Task / Organisation	epSOS / IHE-Europe	Participating Nation (Own development)	F.E.T. (NCP-in-a-T-Box)	Industry (Components)
Test Planning	X			
Test Design	X			
Test Implementation	X	X	X	X
Test Execution		X	X	X
Test Evaluation	X			

epSOS and IHE-Europe

Where epSOS undertakes the development of a system, the accountability falls ultimately under epSOS but the responsibility for its execution can be assumed by epSOS or its sub-contractors / beneficiaries.

In the case of the NCP-in-a-Transparent-Box, the responsibility falls under F.E.T.

In case of OpenNCP, this time the responsibility falls under the adapting PNs and vendors, as OpenNCP itself is not a complete reference implementation, but a set of integrated components that have to be further completed by the adapting PNs / vendors.

As certain decisions pertaining to the division of work have already been taken, these are reflected here.

Test Planning is assumed by epSOS and the beneficiary IHE-Europe.

Test Design is assumed by the beneficiary IHE and epSOS.

Test Implementation is assumed by the beneficiary IHE-Europe.

Test evaluation is assumed by the beneficiary IHE-Europe.

epSOS will provide Participating Nations all necessary Test Stubs, Drivers, Simulators and Validators to realize interoperability testing. See D3.C.1 Appendix B # 6 for some details about the testing tools.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Participating Nations, F.E.T., and Industry

It is not ruled out that the Participating Nations, F.E.T. or the Industry have anything to implement.

Test Execution will be assumed by the Participating Nations, F.E.T. or the Industry.

In addition, Participating Nations, F.E.T. and the industry are responsible for the delivery, installation, configuration and management of their systems during the Projectathon. Additionally, they will be responsible for the execution of test cases and the delivery of all results to the officiating monitors. Furthermore they are responsible for the analysis of problems arising due to testing of their systems against simulators/validators or other systems. The PN should ensure that Health Professionals are part of the team responsible for executing end-to-end functional tests and for evaluating the test results.

Entry Criteria

The following entry criterion applies to all participants of the SIT:

The exit criteria for the Conformance Test phase (pre-Projectathon) have been met.

Exit Criteria

The purpose of the exit criterion is to determine when testing can be halted, but as the duration defines the end of the test there is no need to define a formal exit criterion. At the end of the tests, the results are collected and a final summary report is created and communicated to all participants.

Deliverables

Test Results entered by the Participating Nation / vendor into the Gazelle system (requirement for the Test Evaluation)

A Test Report to be provided by IHE-Europe (through the testing leader in epSOS) for each participating PN or organisation indicating whether or not they have passed the Projectathon and can proceed with the Pre-Pilot tests.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.1.3.6.1 e1-REQ-5213 PAT Grace Period

Immediately after the PAT, when they are back home the participants are allowed to complete unfinished test cases and provide logs remotely for 1 or 2 weeks. The duration is determined according to the observations during the Projectathon. The tests that are completed during this grace period are also taken into account in the PAT reports.

4.1.3.7 e1-REQ-5209 Pre-Pilot Test

Related to e1-REQ-5207 Conformance Test (Pre-Projectathon)

Related to e1-REQ-5216 Interactions among the epSOS test phases

Related to e1-REQ-5220 Conformance Gate 1 (CG1)

Related to e1-REQ-5210 Pre-Projectathon and PPT-slot Test Cases (Conformance Tests)

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Related to e1-REQ-5212 Test Cases for end-to-end Functional Testing

Purpose

The Pre-Pilot Test (also called LSP-Testing) is the phase to regression test the installed components in their target pilot environment firstly as a standalone component and secondly with other standalone components or systems. Finally services are tested in the complete Large Scale Pilot testing infrastructure, separated from the LSP-Operational Infrastructure for safety and security reasons.

Its goal is to ensure that there are no problems or issues with the setup and configuration of the epSOS Infrastructure and the components connected to it. Tests are executed using dummy data, or real patient data that has been anonymized (decision is up to the Participating Nation). A Participating Nation may decide to use real Patient data or real Patients, who require to be informed that they are participating in a pre-pilot trial. Extensive and possibly exhaustive end-to-end testing is performed, involving HPs from Country B, to ensure the level of safety in the document semantic transformation to achieve functional interoperability and get statistically significant data for the Evaluation performed by WP1.2.

Additionally a clinical risk assessment is to be conducted against the original data sent from Country A and the data received by Country B to ensure that during the transformation of data, the unity of the patient data is preserved.

Once a PN has passed this phase and their Pilot fulfils the entry criteria for the LSP Operation, it is able to enter the Trust Domain of epSOS and will be interoperable with all other Pilots that have the same status

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

PAT through LSP Operation

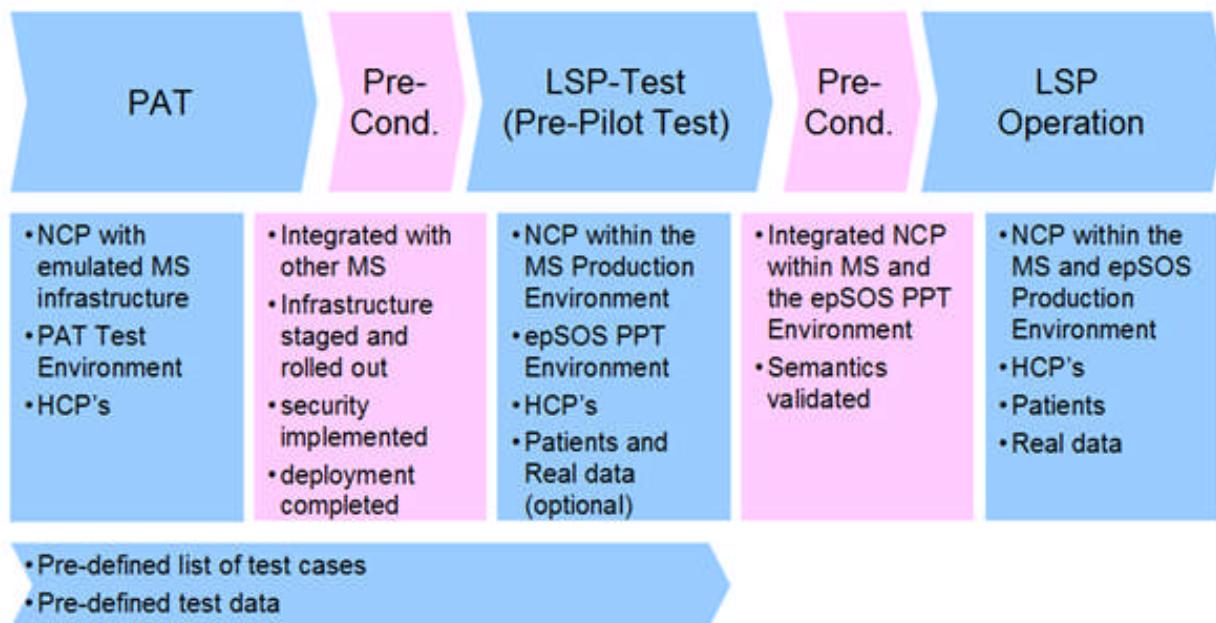


Figure - PAT through LSP Operation

Pre-Pilot Testing is similar to a combination of pre-Projectathon and Projectathon considering the scope of testing activities; i.e. it includes conformance, interoperability and end-to-end functional testing. The main difference is that, the NCP has to be connected to the real national infrastructure, but with virtual data. Its goal is to ensure that there are no problems or issues with the setup and configuration of the pilot environment of a PN. PPT is a “conformance gate” to go into real operation. According to the needs of the PNs, two weeks long PPT slots are organized a few times in a year for completing these tests. However, PPT is a continuous process and the PNs need to operate their testing environments even after starting real operation.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Responsibility

Task / Organisation	epSOS / IHE-Europe	Participating Nation (own Development)	F.E.T. (NCP-in-a-T-Box)	Industry (Components)
Test Planning	X	X		
Test Design	X	X		
Test Implementation	X	X		
Test Execution		X		
Test Evaluation	X	X		

epSOS

The responsibility for the preparation, organisation, evaluation of results, and reporting of this test phase with respect to the NCP lies wholly within epSOS, through IHE-Europe. The end to end tests from the Portal or Participating Nation B National Infrastructure through to the Participating Nation A National Infrastructure will indirectly test all components in the process chain.

The Participating Nations have to maintain a test environment to participate to the Pre-Pilot Testing. The only difference of this test environment from the operational environment should be that the test environment should provide virtual data, not real patient data. This test environment should always be available, even after passing a Pre-Pilot Testing (PPT) slot. PPT is a living process, for example, when there is a change need to be done during operation, it has to be done first on the testing environment, and then transferred to the operational environment.

Together with IHE-Europe, epSOS organizes PPT slots that are formal Pre-Pilot Test execution and verification slots that should normally take 2 weeks. With the exception of the first PPT-slot that took much longer (i.e. six months), epSOS will strictly conform to this 2 weeks deadline for the next PPT-slots. During a PPT-slot, the scope of testing activities to be completed by the PNs are almost identical to the test cases that are executed during Pre-Projectathon and Projectathon phases. Hence, a PPT-slot covers conformance, interoperability and end-to-end functional testing. Also, a PPT-slot is again managed (registration, providing test logs, validating tests, etc.) via the Gazelle Management Tool.

Participating Nations

Participating Nations are responsible for the delivery, installation, configuration and

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

management of their systems during the Pre-Pilot Test phase. Additionally they are responsible for the execution of test cases and the delivery of all results to epSOS through the Gazelle Management tool. Furthermore they are responsible for the analysis of problems arising due to testing of their systems against simulators/validators or other systems.

The PN should ensure that Health Professionals are part of the team responsible for executing end-to-end functional tests and for evaluating the test results.

Entry Criteria

Test Report from the Service Interoperability Test indicating that the Projectathon has been passed.

The PNs have to provide evidence to KT3.C.4 leader and WP3.C leader that they are ready for the PPT-slot through links to validation results in the test simulators provided by Gazelle. These tests will be identical to the pre-Projectathon tests, whose steps are explained here: <http://gazelle.ihe.net/epSOS-doc/>. The PNs are also encouraged to do peer-2-peer tests among themselves, and inform again KT3.C.4 leader and WP3.C leader about the results. Note that this pre-PPT phase is not a formal process managed through Gazelle Management tool and verified by IHE-Europe, but it is still mandatory for making sure that the PNs are actually capable of achieving a PPT-slot.

Exit Criteria

All Test Cases related to standalone (i.e. conformance) tests have been executed and have the test result Pass.

All Test Cases related to interoperability tests have been executed and have the test result Pass.

All Test Cases related to end-to-end functional tests have been executed and have the test result Pass.

The Clinical Risk Assessment presents no adverse risk to patients.

When the defined exit criteria have not been met the Test Report must list the deviations and their estimated risk.

Deliverables

Clinical Risk Assessment.

Test Results entered by the Participating Nation into the Gazelle Management tool (requirement for the Test Evaluation)

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

A Test Report to be provided by epSOS via IHE-Europe for each participating PN indicating whether or not they have passed the Pre-Pilot Test and are able to switch to live operation and enter the Trust Domain of epSOS. The raw results, i.e. a part of this Test Report, is provided automatically by the Gazelle Management tool. The Test Report is to be produced by WP3.10 in epSOS Phase 1 and WP3.C in Phase 2.

4.1.3.7.1 e1-REQ-5214 Pre-PPT Slot

For participation to a PPT-slot, the PNs have to provide evidence to KT3.C.4 leader and WP3.C leader that they are ready for the PPT-slot through links to validation results in the test simulators and validators provided by Gazelle. Furthermore, they have to exchange PS and/or eP/eD documents with all possible counterpart PNs available in the PPT environment and the other PNs who will participate to the same PPT-slot. This pre-PPT-slot phase is not a formal process managed through Gazelle or IHE-Europe, but it is still mandatory for making sure that the PNs are actually capable of achieving a PPT-slot.

4.1.3.7.2 e1-REQ-5215 PPT-Slot

According to the needs and statuses of the PNs, two weeks long PPT-slots are organized a few times in a year for repeating all tests within the scope of pre-PAT and PAT (i.e. conformance, interoperability and end-to-end functional testing) with real national infrastructure and virtual data. PPT-slot is a conformance gate to go into real operation. It is a remote testing activity managed through Gazelle by IHE-Europe and KT3.C.4 PPT leader. Registration through Gazelle® Management tool is necessary as in the case of PAT. It should be noted that the overall PPT phase can be used for debugging and configuration management; however PPT-slot is restricted to testing formally according to the test plan and test cases; it is not for debugging. A PPT-slot is a formal process that leads to accept a PN for the next step (i.e. to go to the real operation).

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

4.1.4 e1-FLD-275 Change management principles

4.1.4.1 e1-TXT-879 Note

During the lifetime of the epSOS Project, some changes in the PN implementations might be required for many reasons. These changes might also affect testing; e.g. they might lead to development and execution of new tests against the updated PN implementations, or only re-execution of existing tests. This depends on the type and scope of the change, which can be a new patch for bug fixing, MVC/MTC update or a brand new service implementation.

The overall objective of the epSOS Project to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes belongs to the epSOS Change Manager (ChM) and the supporting Change Advisory Board (CAB), in which the WP3.C Leader is an active participant. ChM and CAB together manage the change management operation, elaborate on details of change and take decisions with respect to a particular change.

Following further details of change management from the testing strategy point of view are presented in dependence to the type of change.

4.1.4.2 e1-REQ-5265 Implementation of new specifications

- a. When the technical details of the new specifications are provided by WP3.A or by other responsibles such as the Security Expert Group (SEG) (e.g. through EED Design deliverable), WP3.C and testing contractor (i.e. IHE-Europe) MUST analyze the new design specifications. The implementation decisions of WP3.B MUST be taken into account as well.
- b. According to analyses, WP3.C and IHE-Europe MUST decide on whether the new requirements should be covered by new test asset development, update of existing test assets or total re-use of existing test assets.
- c. WP3.C and IHE-Europe MUST do the testing implementation planning accordingly.
- d. IHE-Europe MUST do the implementation and assure the correctness of the implementation through internal testing, according to the agreed planning.
- e. WP3.C, together with the necessary experts such as from SEG or Semantic Task Force Group (TFG), MUST validate the updated and/or new test asset implementation.
- f. IHE-Europe MUST include the updated and/or new test assets into the corresponding epSOS test phases.
- g. In line with the main participation rules presented above, the PNs who have already achieved a PAT previously (including those in operation) and are subject to these newly implemented

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

specifications, MUST proceed with PPT and PPT-slot testing to complete successfully the updated and/or new test assets against their PPT environments.

I. If the PN is already in operation, after it becomes successful with these updated and/or new test assets, it MUST apply the updates done in its PPT environment to its operation environment. The rest is beyond the scope of WP3.C, but it is RECOMMENDED by WP3.C to repeat the same tests in operation environment as well.

h. If the PN has not achieved a PAT yet, then it MUST proceed with its preparations for the next possible PAT, taking into account the updated and/or new test assets.

4.1.4.2.1 e1-TXT-880 Note

If there are new specifications to be implemented, as in the case of new and extended services that are introduced within the scope of epSOS Phase 2, then this will lead to either update of existing test assets or brand new development of test assets, followed by execution of these tests by the PNs and/or vendors.

4.1.4.3 e1-REQ-5266 Changes to NCP configuration, Patches and MVC/MTC updates

a. When the change is a new patch for bug fixing or a configuration change in the NCP, WP3.B MUST provide the details and implementation planning of the change to WP3.C. When the change is MVC/MTC update, Semantic TFG must provide this information to WP3.C.

b. WP3.C and IHE-Europe, in cooperation with the involved experts such as from WP3.B or Semantic TFG, MUST do the analysis and make the relevant updates to the existing test assets if found necessary, in a similar way it is explained in e1-REQ-5265.

c. WP3.C MUST inform the PNs who are already operating a PPT environment, about the test process to be followed. Depending on the details of change, this can be re-execution of some updated tests, or re-execution of existing tests only. The identified tests MUST be performed in the PPT environments of the PNs who are affected by the change. Note that this is an ad-hoc process that has to be realized for each change individually; i.e. it is not possible to fix the set of tests to be repeated in advance.

I. If the PN is already in operation, after it becomes successful with these updated and/or existing test assets, it MUST apply the updates done in its PPT environment to its operation environment. The rest is beyond the scope of WP3.C, but it is RECOMMENDED by WP3.C to repeat the same tests in operation environment as well.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.1.4.3.1 e1-TXT-881 Note

If the change is limited with a configuration change in the NCP, new patch for bug fixing or MVC/MTC update, then it is almost guaranteed that there will be no need for brand new test asset development (in case it turns the opposite way, proceed with e1-REQ-5265). Such changes will lead to either slight update of the existing test assets or re-use of the existing test assets.

4.1.4.4 e1-REQ-5267 PN in operation not implementing phase II services

- a. In case the new design is totally backwards compatible (D3.A.3 - EED Design is planned to be backwards compatible), it is expected that a PN who will not implement any Phase 2 service SHALL NOT be REQUIRED to re-execute the tests. However, for example, if there is a change in content of an existing service (e.g. modification of the patient summary template), then the validators for the PS will be updated, and the old PN MUST re-execute according to these updated validators, first in the PPT environment, and then in the operation environment. Hence, this case becomes identical with e1-REQ-5266.
- b. In case backwards compatibility is not possible with the updated service (e.g. modification of the transactions), then after updating the implementation of the service, the PN MUST proceed with PPT and PPT-slot testing. Hence, this case becomes identical with e1-REQ-5265.

4.1.4.4.1 e1-TXT-882 Note

The third case would appear when a PN from Phase 1 (might be already in operation) decides not to implement any of the Phase 2 services.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2 e1-FLD-252 Logical Perspective

4.2.1 e1-FLD-265 Basic Requirements

4.2.1.1 e1-REQ-5222 Test-Bed actuality and synchronization with epSOS specifications

The test bed and the test suites MUST always be kept updated according to the latest approved epSOS specifications, according to the time plan agreed between WP3.C and Test Bed Provider, taking into account the epSOS Change Management Process. With approval, Project Steering Board (PSB) approval is RECOMMENDED; but in the worst case Technical Project Management (TPM) approval MUST be ensured. When there are updates in existing specifications, in order to ease the adaptation of the test bed and the test suites, the changes MUST be clearly identified. WP3.C Validation in cooperation with WP3.A Architecture, WP3.B Implementation and TPM MUST provide the correct versions of the specifications to the test bed provider.

4.2.1.2 e1-REQ-5223 epSOS testing scope

epSOS testing MUST be focused on cross-border data exchange, hence the NCP to NCP communication.

4.2.1.2.1 e1-TXT-870 Note

In addition, epSOS testing includes end-2-end functional testing, semantic and document validation, and existence and formal compliance testing of audit trails / security provision as well. On the other hand, although NCP-to-NCP testing (including end-2-end testing) might reveal issues related with NCP to National Infrastructure communication on one side, or on both sides, this is not the main objective of epSOS testing.

4.2.1.3 e1-REQ-5224 Monitors' knowledge of specifications

The monitors (i.e. human testing experts) that are provided by the test bed provider MUST have, as a whole, thorough knowledge of the epSOS specifications well before any physical or online testing activity.

4.2.1.4 e1-REQ-5225 Test efficiency

Although fine-grained test suites for testing very simple transactions SHOULD be in place, in general, the test bed and the test suites MUST always test as much as possible in a single step, to reduce efforts on the testers' and also on the validators' (i.e. monitors) side.

 epSOS <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.1.4.1 e1-TXT-883 Test efficiency example

For example, while testing a patient summary retrieval transaction implemented via IHE XCA (hopefully XCF For example, while testing a patient summary retrieval transaction implemented via IHE XCA, the test bed MUST perform validation checks at the messaging layer (SOAP header, security assertions in the SOAP header, SOAP body, SOAP attachments), at the document layer (structural validation of the PS document, semantic validation of the PS document) and also related with secure communication (i.e. use of certificates over HTTPS and establishment of the VPN communication) at once. The testers MUST NOT be forced to do several tests via several different test components/interfaces as in the case of epSOS Phase 1 testing process, while all can be done in a single test execution.

4.2.1.5 e1-REQ-5227 Interoperability testing

epSOS testing MUST NOT be limited to only conformance testing against some simulators; it MUST also include interoperability testing. When using a non-secure communication mode (no VPN and TLS) or a limited secure mode (TLS with private keys shared with the test bed in advance), the test bed MUST have the capability to listen the communication among the SUTs and automatically perform validation checks on the intercepted messages. Ideally, the message capture SHOULD NOT interfere with the way the SUTs interoperate as they would under real business conditions. The test bed MUST benefit from the already existing validation facilities at the messaging and document layer for realizing interoperability testing.

4.2.1.5.1 e1-REQ-5228 Interoperability testing requirement

According to GITB, the three most common ways to capture message traffic between SUTs are:

- a) Using a “man-in-the-middle” system operating and re-routing messages at transport level (e.g. an HTTP proxy or a TCP intermediary). This is typically the least intrusive approach, although it imposes restrictive conditions (the messages and sessions MUST NOT be encrypted; or if they are encrypted, the test bed as the intermediary MUST have the necessary private keys to decrypt them).
- b) Instrumenting of one of the SUT so that message capture is performed at the endpoint, e.g. on the message handler of the SUT. Later on this message capture can be consolidated in a Test Execution Log.
- c) Configuring the sending SUT(s) so that they duplicate messages sent and forward a copy a Monitoring component or directly to the Test Bed.

 <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Ideally, the message capture SHOULD NOT interfere with the way the SUTs interoperate as they would under real business conditions. Therefore, the best alternative in the above list is a).

The test bed MUST benefit from the already existing validation facilities at the messaging and document layer for realizing interoperability testing. Therefore, the main issue to be concentrated here is the automatic capturing of the communication between SUTs, by at most requesting the SUTs to change their endpoints for sending the messages; i.e. a SUT can send a message to the test bed which then forwards this message to the intended SUT, instead of directly sending the message to the intended SUT.

The test bed and the interoperability test suites MUST provide the testers necessary configuration options via a GUI.

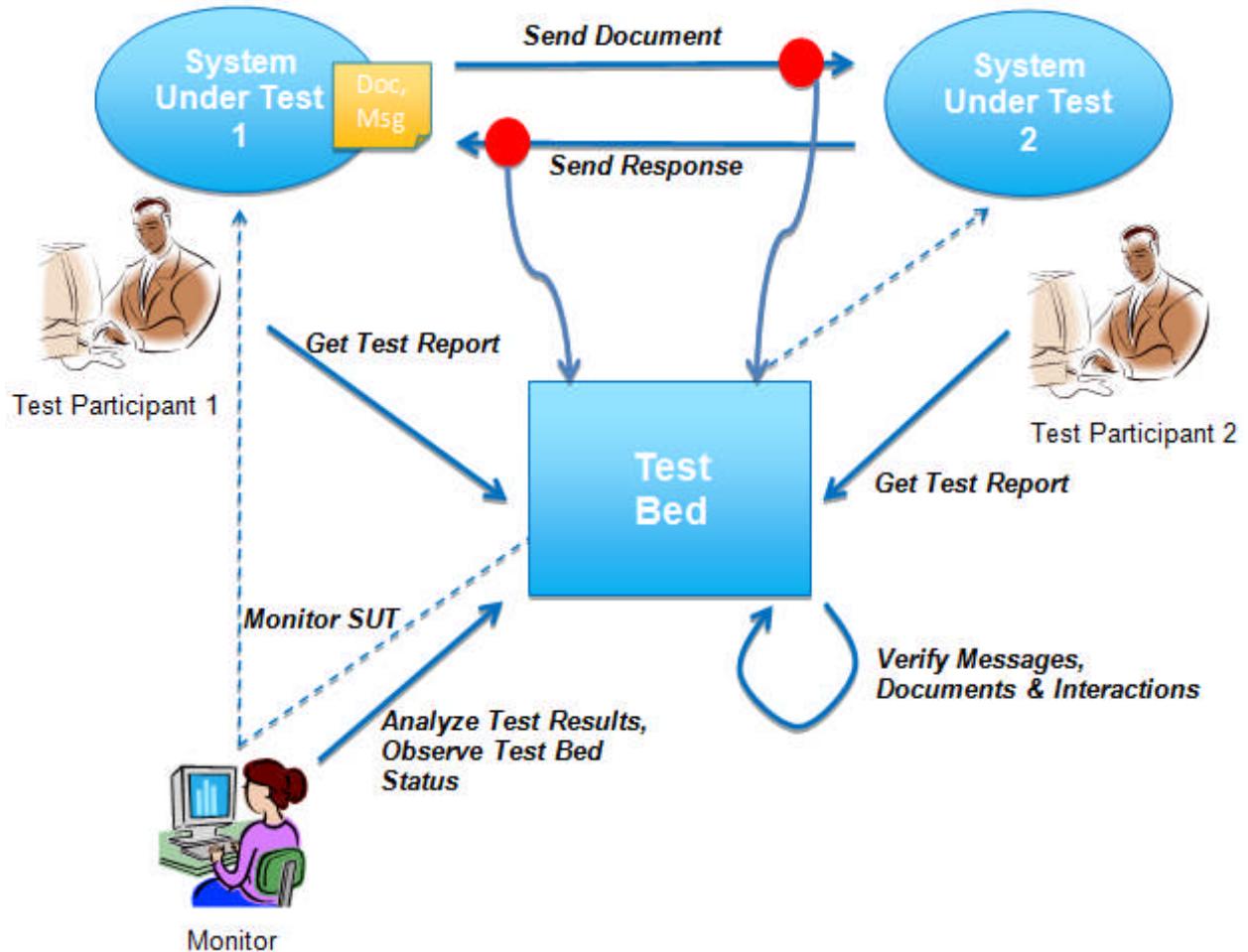
4.2.1.5.1.1 e1-TXT-877 Note

According to GITB, the three most common ways to capture message traffic between SUTs are:

- a) Using a “man-in-the-middle” system operating and re-routing messages at transport level (e.g. an HTTP proxy or a TCP intermediary). This is typically the least intrusive approach, although it imposes restrictive conditions (the messages and sessions should not be encrypted).
- b) Instrumenting of one of the SUT so that message capture is performed at the endpoint, e.g. on the message handler of the SUT. Later on this message capture can be consolidated in a Test Execution Log.
- c) Configuring the sending SUT(s) so that they duplicate messages sent and forward a copy a Monitoring component or directly to the Test Bed.

The following figure presents briefly how automatic capturing of message exchange between the SUTs, and then automatic validation of the captured messages, documents and interactions can be done.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013



4.2.1.6 e1-REQ-5229 Assurance of patient safety

epSOS testing MUST assure patient safety. Hence, focus MUST be set on semantic transformation, CDA document scrutiny and end-2-end functional testing as being of extreme relevance to assess the robustness with respect to patient safety protection.

4.2.1.7 e1-REQ-5230 Assurance of security & privacy

epSOS testing MUST assure information security, privacy rights and full compliance to the data protection regulations. Hence, security robustness is an attribute of the SUT that MUST be covered by testing procedures, including the correctness of non-repudiation functionalities.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

4.2.2 e1-FLD-266 Engineering Level Requirements

4.2.2.1 e1-TXT-872 Note

This section focuses on engineering (i.e. technical) level requirements of the test bed to be used in epSOS. The main categories in this section are:

Document Layer Validation Requirements

Messaging Layer Validation Requirements

Business Process (Workflow) Layer Validation Requirements

Interoperability Testing Requirements

Common Technical Requirements of the Test Bed

4.2.2.2 e1-FLD-268 Document layer validation requirements

4.2.2.2.1 e1-REQ-5231 Syntax & structure validation

The test bed MUST perform document syntax and structure validation of the epSOS electronic documents, i.e. electronic Patient Summary (ePS), ePrescription, eDispensation, eConsent, Audit message (which can be considered a document in epSOS context) and any further documents to be designed during the second phase of epSOS, according to the related structured document schemas.

4.2.2.2.1.1 e1-TXT-873 Note

For example such as the XSD of HL7 CDA R2

4.2.2.2.2 e1-REQ-5232 Semantic validation

The test bed MUST perform semantic validation of the epSOS electronic documents according to the content templates and business rules that are defined within the epSOS specifications on top of the common schemas of the used standards. The restrictions that are defined verbally in these content templates and business rules MUST be expressed in a machine executable way by the test bed provider and validated by epSOS experts responsible for related epSOS specifications. Since all epSOS documents are XML-based, the RECOMMENDED way of expressing these business rules is using Schematron or model-based validators.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

4.2.2.2.1 e1-REQ-5233 Mandatory/optional attribute validation

The test bed MUST validate mandatory/optional attribute constraints, which are defined by epSOS content templates and business rules in addition to similar constraints in the XSDs.

4.2.2.2.2 e1-REQ-5234 Coded concept validation

The test bed MUST check whether the coded data fields comply with the defined epSOS value sets and additional vocabularies. Validation MUST cover code and code system identifier attributes; in case the attributes for code system name and designation are included in validation, they MUST be case insensitive.

4.2.2.3 e1-FLD-269 Messaging layer validation requirements

4.2.2.3.1 e1-REQ-5235 Conformance of communication

The test bed MUST perform validation of the exchanged messages according to the used messaging protocol. In epSOS, currently all communication among NCPs is done via SOAP Web Services. The test bed MUST be able to check conformance of NCP communication according to the Web Service specifications as restricted by the preferred interoperability profiles such as IHE XCPD, XCA, XDR and XUA. These profiles define both structural and semantic requirements, all of which MUST be covered.

4.2.2.3.1.1 e1-REQ-5236 SOAP header validation

The test bed MUST check whether the SOAP header is valid. This also involves checking the syntactic and semantic validity of the security/privacy assertions (i.e TRC assertion, HCP assertion) that are exchanged within the WS-Security headers.

4.2.2.3.1.2 e1-REQ-5237 SOAP body validation

The test bed MUST check whether the SOAP body is valid. The structural and semantic validity of the SOAP body MUST be checked.

4.2.2.3.1.2.1 e1-TXT-874 Note

In some transactions such as XCPD or XCA:list responses, all the requested information is presented directly within the SOAP body.

4.2.2.3.1.3 e1-REQ-5238 SOAP attachment validation

If utilized by an interoperability profile, the test bed MUST check whether the SOAP attachment(s) are valid. As explained in e1-REQ-5225 (i.e. test efficiency), after getting the

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

attachment, the messaging layer MUST call the document layer validation facilities for a complete structural and semantic validation of the document.

4.2.2.3.1.3.1 e1-TXT-875 Note

In some transactions such as XCA:retrieve, the requested patient document is transported as a SOAP attachment.

4.2.2.3.2 e1-REQ-5239 Validation of secure communication

The test bed MUST check compliance to secure communication requirements as defined by the epSOS specifications, i.e. use of security certificates over HTTPS and establishment of the IPsec VPN connection.

4.2.2.4 e1-FLD-270 Business process (workflow) layer validation requirements

4.2.2.4.1 e1-REQ-5240 Automated workflow testing

The test bed MUST be able to perform automated workflow (i.e. business process) tests. Such workflows will be defined by epSOS.

4.2.2.4.1.1 e1-TXT-876 Note

An example workflow constitutes of the following steps: identification of the patient, defining remote consent, patient summary document query and patient summary document retrieval.

4.2.2.4.2 e1-REQ-5241 Workflow execution

The test bed MUST ensure the sequence of steps that need to be realized for a workflow, and wait for relevant requests/responses from the SUT, or send relevant requests/responses to the SUT. The status of the workflow execution MUST be presented to the tester, who can be a technical person or health professional according to the workflow definition, via graphical user interface (GUI).

4.2.2.4.3 e1-REQ-5271 Reuse of existing test resources

At the workflow layer, the test bed MUST benefit from the already existing validation facilities at the messaging and document layers. Again, this MUST be in line with requirement e1-REQ-5225 (i.e. test efficiency).

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.2.2.5 e1-FLD-272 Common technical requirements of the test bed

4.2.2.5.1 e1-REQ-5242 Registration of testers

The test bed MUST provide the capability to the testers to register themselves and their SUTs for testing activities. There MUST be testing sessions dedicated to epSOS testing activities.

4.2.2.5.1.1 e1-REQ-5243 Alternative user authentication means

The test bed MAY allow Open ID and STORK eID integration for testing accounts.

4.2.2.5.2 e1-REQ-5272 Accessibility of test suites

The test suites MUST be clearly identified and easy to locate and initiate. In case the location of a test suite changes, then all previous links pointing to it MUST be updated and informed to the testers immediately.

4.2.2.5.3 e1-REQ-5244 Interaction with tester

The test bed MUST have the ability to inform the tester about the testing steps to be executed within a test suite, before initiating that test suite. Testers MUST be offered a test suite description that can be narrative text or some graphical representation describing the test suite flow and each step, also explaining any required information from the tester or the SUT before starting the execution of the test. For complex workflows, it is RECOMMENDED to have a notification mechanism (over the user interface) that informs the tester about the status of execution.

4.2.2.5.4 e1-REQ-5245 Adaptive test execution parameters

The test bed MUST provide a mechanism to ask the testers some necessary parameters and information about their SUTs before starting test execution; related to network configuration, security configuration or some epSOS service specific configuration such as providing home community id of a PN.

4.2.2.5.4.1 e1-TXT-878 Note

For example parameters such as providing home community id of a PN.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

4.2.2.5.4.2 e1-REQ-5273 Binding automation

This mechanism MUST automatically bind the information into the test suite without any manual intervention so that the corresponding message/document elements can be tested if they are consistent with provided information.

4.2.2.5.4.3 e1-REQ-5274 Minimalist approach

Such configuration parameters requested from the testers MUST be kept at minimum.

4.2.2.5.4.4 e1-REQ-5275 Remembering configuration parameters

For ease of use, it is RECOMMENDED that the GUI of the test bed remembers previously provided configuration parameter values, at least the last ones, across testing sessions (session as in user session utilized in Web applications, not epSOS test sessions such as projectathon). In parallel, it is also RECOMMENDED that the testers enter their SUT configuration once for an entire testing session and the configurations are bound to the testing sessions.

4.2.2.5.5 e1-REQ-5246 Exchange of SUT configurations

Both interoperability and conformance test scenarios necessitate some configurations regarding SUTs. The test bed SHOULD enable testers to share configuration parameters of their SUTs among each other.

4.2.2.5.6 e1-REQ-5247 Reporting of results

The test bed MUST have a reporting mechanism that clearly informs the testers about the results of the testing executions they had.

4.2.2.5.6.1 e1-REQ-5248 Summary view

The test report MUST have a summary view presenting the overall success/failure status of the fine-grained test steps.

4.2.2.5.6.2 e1-REQ-5249 Accessibility of report details

The testers SHOULD be able to access parts of a test report easily, in which details about the results of a test step are presented.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.2.5.6.3 e1-REQ-5250 Error location and evidence

The test report MUST clearly point to the location of any error of the SUT, supporting it with evidence about the error.

4.2.2.5.6.4 e1-REQ-5251 Error resolution guidance

In case of presence of an error detected in the SUT(s), the test report SHOULD also provide information, as much as possible, on how to resolve that error.

4.2.2.5.6.5 e1-REQ-5252 Error severity classification

Severity of the detected errors SHOULD be included in the test report.

4.2.2.5.6.5.1 e1-TXT-884 Note

Defect severity classification is explained in Section 3.6.3.1 of D3.C.1 Appendix-B.

4.2.2.5.7 e1-REQ-5253 Utilization of a test definition language

In order to facilitate easy maintenance of the test cases and test suites, the test bed SHOULD adapt a structured test definition language for defining the test cases and test suites. The test bed SHOULD be able to automatically execute instances conforming to this test definition language.

4.2.2.5.8 e1-REQ-5254 History view

The test bed MUST provide a history view to the testers providing the complete history of test executions for their registered SUTs. This view MUST provide basic statistics as well. At any time, it MUST be possible to see the detailed test report of a specific test execution.

4.2.2.5.9 e1-REQ-5255 Management GUI

Similar to the history view provided to the testers, the test bed MUST also provide a management GUI to be used by monitors of the test bed provider and authorized persons in epsOS (e.g. coordinator, WP3.C leader, etc.; to be decided). The management GUI MUST provide the testing history of all the SUTs supported with basic statistics and the functionality to access the details of any test execution by any SUT. User friendly filtering mechanisms SHOULD be in place

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.2.2.5.10 e1-REQ-5256 Versioning

Test bed, test suites, their significant parts such as schematrons and test data MUST be versioned. The version MUST be visible to the testers in the GUI and for each version there SHOULD be a statement to which version of epSOS specification it corresponds and a log of changes since the last version.

4.2.2.5.11 e1-REQ-5257 Validation of the test bed by experts

The test bed MUST be validated by experts responsible for the relevant specification before each testing session, in case a major revision in specification or test bed was done since the last testing session. The validation SHOULD be done, e.g., by testing with the reference implementation (in epSOS Phase 1), systems of PNs that have already achieved a PPT-slot or reference set of documents. The test report from this validation MUST be made available to the testers.

4.2.2.5.12 e1-REQ-5258 Linking with requirement/issue management tools

The test bed MAY have linking functionality to some issue management tools such as Redmine and JIRA, and requirement management tools such as Contour, which are used by epSOS as well.

4.2.2.5.13 e1-REQ-5276 API availability

The test bed MAY have linking functionality to some issue management tools such as Redmine and JIRA, and requirement management tools such as Contour, which are used by epSOS as well.

4.2.3 e1-FLD-267 Sustainability Requirements

4.2.3.1 e1-FLD-273 Process sustainability

4.2.3.1.1 e1-REQ-5259 Compliance validation by independent bodies

In line with the implementation strategy defined in D3.B.1 and the sustainability strategy under definition in WP2.2, which foresees an independent growth of vendors and PN level solutions, the procedure of validating the compliance of NCPs and components to the epSOS specification SHOULD become more and more a task assigned to an independent body that can organise and manage test events open to all, and provide validation of conformity.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

4.2.3.1.2 e1-REQ-5260 Sustainability of test procedures and events

Test procedures and events SHOULD become self-sustainable with the attendees paying their registration fees fully or partially, in order to free them from the need of project funding.

4.2.3.2 e1-FLD-274 Test bed sustainability

4.2.3.2.1 e1-REQ-5261 Compliance to an interoperability testing framework

epSOS testing strategy and the test bed to be used in epSOS SHOULD be compliant with an internationally recognized interoperability testing framework.

4.2.3.2.2 e1-REQ-5262 Proven experience of test bed provider

The test bed provider MUST be capable from the technical and global organizational point of view. They MUST have experience in this area, proven with previously organized similar physical and online interoperability testing events.

4.2.3.2.3 e1-REQ-5263 Long term availability of epSOS testing resources

epSOS test suites and the test bed SHOULD be available after the end of epSOS project, i.e. after 2013. It is also RECOMMENDED that such testing resources are available as part of the regular work of the test bed provider; not only as a derivative.

4.2.3.2.4 e1-REQ-5264 Documentation of testing facilities

The test bed provider MUST provide guideline documents and also videos for using the testing facilities provided by the test bed and test suites.

4.2.4 e1-FLD-264 Detailed Participation Criteria for the Test Phases (Conformance Gates)

WP3.9, WP3.10, WP4.3 in epSOS Phase 1 and WP3.C, KT1.4.10, WP4.C in Phase 2 have defined several technical / semantic detailed participation criteria for the epSOS test phases. These are also known as Conformance Gates. There are three Conformance Gates, and they are incremental; i.e. each one is built upon the previous one, and further extends the previous. The Conformance Gates are formally released in the PN_Report Check List (managed by PD4, specifically WP4.C). NEPCs are requested to provide the updated status of their check list fulfilment every two weeks.

In this part, the Technical and Semantic Conformance Gates that are relevant for testing are

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

provided. For the formal and complete list of Conformance Gates, please refer to the PN_Report Check List.

4.2.4.1 e1-TXT-869 Note

WP3.9, WP3.10, WP4.3 in epSOS Phase 1 and WP3.C, KT1.4.10, WP4.C in Phase 2 have defined several technical / semantic detailed participation criteria for the epSOS test phases. These are also known as Conformance Gates. There are three Conformance Gates, and they are incremental; i.e. each one is built upon the previous one, and further extends the previous. The Conformance Gates are formally released in the PN_Report Check List (managed by PD4, specifically WP4.C). NEPCs are requested to provide the updated status of their check list fulfilment every two weeks.

In this part, the Technical and Semantic Conformance Gates that are relevant for testing are provided. For the formal and complete list of Conformance Gates, please refer to the PN_Report Check List.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.2.4.2 e1-REQ-5219 Conformance Gate 0 (CG0)

Related to e1-REQ-5207 Conformance Test (Pre-Projectathon)

Related to e1-REQ-5217 Main participation rules for test phases

Related to e1-REQ-5208 Service Interoperability Test (Projectathon)

A participant has to pass Conformance Gate 0 (CG0) to be allowed to participate to a pre-PAT and PAT. CG0 criteria are as follows:

Participants MUST create and formally approve the Master Translation and Transcoding Catalogue (MTC), verifying all the agreements / contracts with the relevant Standard Development Organizations (SDOs) are fulfilled.

The participants that use Transformation Manager (including Terminology Service Access Manager [TSAM], TSAM Synchronizer and Local Terminology Repository [LTR]) for transcoding / translation MUST upload their MTC to eCRTS (at present HealthTerm) and MUST synchronize their Local Terminology Repository (LTR) with eCRTS. In case a participant is not using Transformation Manager for transcoding / translation, but using its own solution, then this participant MUST prove to the epSOS semantic experts during and after PAT that this solution is technically correct and terminology validation procedures are in place to prevent clinical safety risks.

Participants MUST integrate their NCP at least with a virtual National Infrastructure (i.e. a simulated NI), and if possible with the real National Infrastructure with virtual data.

Participants MUST create the Critical Test Data (CTD) and OPTIONALLY Representative Test Data (RTD) and load them in their virtual National Infrastructures; i.e. CTD is a MUST, and RTD is RECOMMENDED.

Participants MUST provide the credentials for the CTD and RTD.

Participants MUST run scrutiny tests on these CTD and RTD.

If acting as Country B, participants SHOULD translate Portal-B in Country-B language.

Participants MUST request and install certificates. They are allowed to participate with self-signed certificates, which MUST be still compliant with epSOS specifications in terms of content.

Participants MUST use central services (i.e. TSL Editor, SyncApp) to create and upload their configuration files to the epSOS central config area. The config area that is used for both PPT and PAT MUST be used.

Participants MUST enable TSL synchronizer in their NCP setup.

Participants MUST establish VPN communication as used in the PPT environment.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Participants SHOULD successfully exchange at least one document (i.e. complete a workflow of PS and/or eP/eD according to the services that they implement) with each possible counterpart PN available in the PPT environment, and also with the PNs who will be in the same PPT session. The participants MUST inform WP3.C leader about the results.

Participants MUST prepare their HPs for end-to-end functional testing to take place during PAT. HPs MUST register themselves for the electronic questionnaire that is available at <http://gazelle.ihe.net/content/epsos-cda-evaluation-form> and MUST study the questionnaire before PAT.

Participants MUST complete their registration in Gazelle on time, based on the epSOS services they implement.

Participants MUST participate to the Gazelle education teleconference organized by IHE-Europe prior to a PAT.

Participants MUST be able to easily locate and manipulate the application logs of their NCPs, which will be necessary during testing in PAT.

4.2.4.3 e1-REQ-5220 Conformance Gate 1 (CG1)

Related to e1-REQ-5217 Main participation rules for test phases

Related to e1-REQ-5209 Pre-Pilot Test

A participant has to pass Conformance Gate 1 (CG1) to be allowed to participate to a PPT-slot. CG1 criteria are presented below, but before that, there are also some basic criteria to be part of PPT (be careful, not PPT-slot) in general for performing experiments with other PNs in the PPT area for debugging, configuration management, quality improvement, etc. These basic criteria can be termed as pre-CG1, and are listed below:

Participants MUST have passed CG0.

Participants SHOULD have passed a PAT. If not, they MUST have completed all the related pre-PAT tests (i.e. Conformance tests epSOS-1 to epSOS-11).

NCP SHOULD be connected to the real National Infrastructure with virtual data.

The CG1 criteria that must be fully met to be admitted to a PPT-slot are as follows:

Participants MUST have passed a PAT. No Severity 1 and 2 defects (D3.C.1 Appendix-B, # 3.6.3.1) MUST have been detected.

Participants MUST have resolved any issues that were detected in their implementation in previous test phases.

NCP MUST be connected to the real National Infrastructure with virtual data.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

Participants MUST create both CTD and RTD, and make them available in their National Infrastructures.

If acting as Country-B, participants MUST translate and validate Portal-B in Country-B language.

Participants MUST request and install certificates that are totally compliant to epSOS specifications. Self-signed certificates are not accepted.

Participants MUST provide evidence to KT3.C.4 leader and WP3.C leader that they are ready for the PPT-slot through links to validation results in the test simulators and validators provided by Gazelle® Management tool. These tests will be identical to the pre-PAT tests (i.e. Conformance tests epSOS-1 to epSOS-11). Please note that this pre-PPT-slot phase is not a formal process managed through Gazelle® Management tool or IHE-Europe, but it is still mandatory for making sure that the PNs are actually capable of achieving a PPT-slot.

Participants MUST successfully exchange at least one document (i.e. complete a workflow of PS and/or eP/eD according to the services that they implement) with each possible counterpart PN available in the PPT environment, and also with the PNs who will be in the same PPT-slot. The participants MUST inform KT3.C.4 leader and WP3.C leader about the results, again within the scope of pre-PPT-slot activities.

Participants MUST complete their registration in Gazelle® Management tool on time, based on the epSOS services they implement, this time for the PPT-slot.

Organizational aspects MUST be established.

Basic legal requirements MUST be fulfilled.

4.2.4.4 e1-REQ-5221 Conformance Gate 2 (CG2)

Related to e1-REQ-5217 Main participation rules for test phases

A participant has to pass Conformance Gate 2 (CG2) to be allowed to enter into operation. CG2 criteria are as follows:

Participants MUST have passed a PPT-slot. No Severity 1 and 2 defects (D3.C.1 Appendix-B, # 3.6.3.1) MUST have been detected.

Legal, security and organizational requirements MUST be fulfilled.

Once a PN has passed successfully PPT-slot tests and fulfils all entry criteria for the operation environment (CG2), PSB is asked to admit the national pilot to Operation (OP). The pilot then enters LSP OP, i.e. the Trust Domain of epSOS, and is interoperable with all other national pilots.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.5 e1-FLD-257 Test Items

4.2.5.1 e1-TXT-866 Note

The following lists those features found in input specifications that need to be tested, as well as those that cannot be tested.

In the case that requirements cannot be tested the justification is described. The features to be tested are restricted to the NCP and Portal. Requirements relating to the national Infrastructures cannot be tested by epSOS, but such testing is a pre-requisite for each PN.

The features to be tested can be located in the functional service requirements of ePrescription/eDispensation (D3.1.2) and Patient Summary (D3.2.2) services accordingly.

4.2.5.2 e1-FLD-259 Patient Summary

4.2.5.2.1 e1-REQ-5147 HP-B Identification and Authentication

Tested by e1-REQ-3863 HP-B Identification and Authentication

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5176 HP-B Identification and Authentication

Despite being a national implementation it belongs to the processes Electronic Prescribing, Electronic Dispensing and Patient Summary and can be visually validated at the HP-B.

4.2.5.2.2 e1-REQ-5148 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Tested by e1-REQ-3869 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5178 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Validation is restricted to the interface NCP-B to NCP-A. Trust establishment between two different PNs depends on their decision from the legal/organizational perspective. Trust can be established mutually between two countries, with the technical implementation proposed by epSOS. The HP does not play a role in the establishment of the trust relationship, but is affected by its outcome, for example a patient from a country whereby no trust relationship exists. The NCP-B in this case must be prepared for such a scenario.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

4.2.5.2.3 e1-REQ-5149 Patient Identification

Tested by e1-REQ-3868 Patient Identification

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5177 Patient Identification

NCP-B will send a Patient identification request to the NCP-A, which in turn will forward the request to the National Infrastructure of PN A. The NCP-A will receive the Patient Identification data from the PN A National Infrastructure and forward it to the NCP-B. Testing is restricted to validating according to epSOS requirements, that a patient can be identified through the Portal or the National Connector of the NCP-B, and the epSOS interface of the NCP-A. This can be validated visually at the HP-B.

4.2.5.2.4 e1-REQ-5166 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Tested by e1-REQ-3889 Willful Disclosure (Data Confidentiality)

Synchronized with e1-REQ-5194 Willful Disclosure (Data Confidentiality)

It is assumed that an unauthorised party is anyone other than the HP. It will be verified that patient data cannot be obtained through malicious or non-malicious methods within the NCP. epSOS will not verify that patient data in systems other than the NCP can be obtained through malicious or non-malicious methods.

4.2.5.2.5 e1-REQ-5150 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Tested by e1-REQ-3866 Willful Provisioning of Data (»Consent-1«)

Synchronized with e1-REQ-5179 Willful Provisioning of Data (»Consent-1«)

NCP-B will send a Patient Consent request to the NCP-A, which in turn will forward the request to the National Infrastructure of PN A. The NCP-A will receive the Patient Consent answer provided / not provided from the PN A National Infrastructure and forward it to the NCP-B. Testing is restricted to validating according to epSOS requirements, that consent to access patient data can be granted through the Portal or the National Connector of the NCP-B, and the epSOS interface of the NCP-A. It will be possible to conduct the test from the connector side of the NCP-B via the NCP and the Portal along with a visual validation at the HP-B.

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.2.5.2.6 e1-REQ-5170 Authorized Exchange of Data (»Consent-2«; PIN)

Tested by e1-REQ-3867 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5180 Authorized Exchange of Data (»Consent-2«; PIN)

epSOS will verify that the NCP is not accessible via any of its interfaces to anyone other than authorised persons.

The description of this requirement does not refer specifically to the NCP but generally to systems. This requirement therefore encompasses all systems in the end to end process. It is not possible for epSOS to verify systems other than the NCP.

4.2.5.2.7 e1-REQ-5151 Structured Information and Semantic Compliance

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Tested by e1-REQ-3865 Structured Information and Semantic Compliance

Synchronized with e1-REQ-5181 Structured Information and Semantic Compliance

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.2.8 e1-REQ-5152 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Tested by e1-REQ-3871 Semantic Interoperability of Structured Clinical Content

Synchronized with e1-REQ-5182 Semantic Interoperability of Structured Clinical Content

It has to be tested that the initial information in Country A and the received information in Country B are equivalent along the entire process. The final step is a visual validation at the HP-B.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3	Date:	31/01/2013

4.2.5.2.9 e1-REQ-5154 FR19: Patient Summary of Country A available

Tested by e1-REQ-3861 FR19: Patient Summary of Country A available

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.2.10 e1-REQ-5153 Minimum and Maximum Data Sets

Tested by e1-REQ-5131 Minimum and Maximum Data Sets

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5183 Minimum and Maximum Data Sets

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.2.11 e1-REQ-5174 Peering Original Document

Tested by e1-REQ-5133 Peering Original Document

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.2.12 e1-REQ-5163 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Tested by e1-REQ-3872 Traceability and Exercise of Patient Information Rights

Synchronized with e1-REQ-5184 Traceability and Exercise of Patient Information Rights

It is assumed that all systems are responsible for auditing data (NCP-A, NCP-B, and Portal). epSOS will verify that all access or attempted access to medical data via the NCP is audited. This is restricted to the NCP-A and NCP-B. epSOS will not verify the traceability of information stored on systems other than the NCP.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.5.2.13 e1-REQ-5201 FR21: Patient Summary Conformance

Tested by e1-REQ-3892 FR21: Patient Summary Conformance

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.2.14 e1-REQ-5202 FR22: Uniqueness of Patient Summary

Tested by e1-REQ-3893 FR22: Uniqueness of Patient Summary

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that only one Patient Summary is displayed per patient.

4.2.5.2.15 e1-REQ-5203 REQ 3.3.14 Medication Summary only accessible as part of Patient Summary

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Tested by e1-REQ-4599 REQ 3.3.14 Medication Summary only accessible as part of Patient Summary

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.2.16 e1-REQ-5164 Data Integrity

Tested by e1-REQ-3888 Data Integrity

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5186 Data Integrity

Secure communication between NCP's will be verified during interoperability testing. epSOS will verify that the NCP A and B have not damaged, reduced or altered the data in anyway.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.5.2.17 e1-REQ-5167 NFR05 - Access control

Tested by e1-REQ-3880 NFR05- Access control

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5188 NFR05 - Access control

epSOS will verify that the NCP is not accessible via any of its interfaces to anyone other than authorised persons. It is not possible for epSOS to verify systems other than the NCP.

4.2.5.2.18 e1-REQ-5168 Data Origin and Data Authenticity

Tested by e1-REQ-4411 Data Origin and Data Authenticity

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5189 Data Origin and Data Authenticity

Can only be tested between the NCPs.

4.2.5.2.19 e1-FLD-260 Features not to be tested

The following features have a functional aspect that do not relate to the functionality between two NCPs, but between an NCP and its respective national infrastructure or its HP. As epSOS does not test the interfaces within the national infrastructures, it is regarded as outside of the scope of this test strategy.

4.2.5.2.20 e1-REQ-5169 NFR01 - Service availability

Tested by e1-REQ-3876 NFR01- Service availability

Synchronized with e1-REQ-5185 NFR01 - Service availability

The description relates to operational requirements, the result of which would be the definition of SLA's, and the setting up of a Command Centre responsible for monitoring all systems that are connected directly to the epSOS Infrastructure. It is assumed that epSOS will not create a command centre but allow the PN to regulate themselves.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.5.2.21 e1-REQ-5165 NFR03 - Response time

Tested by e1-REQ-3878 NFR03- Response time

Synchronized with e1-REQ-5187 NFR03 - Response time

The response time of an NCP and the response time between NCPs will be verified to be within the defined parameters. This will be restricted to proving that the roundtrip time between the Portal, NCP-B and NCP-A is not excessively slow. The response time of the PN National Infrastructure will not be measured.

This does not cover the response time of any Country B system other than the NCP, or any other Country A system other than the NCP. However, end-to-end response time will be measured for service evaluation purposes.

4.2.5.2.22 e1-REQ-5175 NFR09 - Trust between countries

Tested by e1-REQ-4564 NFR09- Trust between countries

Synchronized with e1-REQ-5190 NFR09 - Trust between countries

This requirement concerns itself with the non-functional aspect of trust between countries, specifically those policies defined by epSOS and to be implemented by the Participating Nations. The implementation of those policies will be verified through Audits during and post rollout.

4.2.5.2.23 e1-REQ-5171 NFR10 - Guaranteed delivery

Tested by e1-REQ-3885 NFR10- Guaranteed delivery

Synchronized with e1-REQ-5191 NFR10 - Guaranteed delivery

epSOS cannot verify that the HP-B confirms that the data is properly received.

4.2.5.2.24 e1-REQ-5172 NFR11 - Single session

Tested by e1-REQ-3886 NFR11- Single session

Synchronized with e1-REQ-5192 NFR11 - Single session

This is a requirement of a PN. This type of functionality must be restricted to the PN national infrastructure and not the NCP. It must already be standard within a PN national infrastructure as this problem could already occur within their borders.

 epSOS <small>EUROPEAN PATIENTS SMOOTH OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
D5.2.3		Date:	31/01/2013

4.2.5.2.25 e1-REQ-5173 NFR12 - Supervision services

Tested by e1-REQ-3887 NFR12- Supervision services

Synchronized with e1-REQ-5193 NFR12 - Supervision services

This concerns operational services and as such is out of scope of epSOS.

These services cover the creation of SLAs and probes, the monitoring of real time performance and services. It is the responsibility of the operational organisations to verify these requirements. This is also coupled with NFR01 – Service Availability.

4.2.5.3 e1-FLD-258 eP/eD

4.2.5.3.1 e1-REQ-5180 Authorized Exchange of Data (»Consent-2«; PIN)

Synchronized with e1-REQ-5170 Authorized Exchange of Data (»Consent-2«; PIN)

Tested by e1-REQ-4542 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

epSOS will verify that the NCP is not accessible via any of its interfaces to anyone other than authorised persons.

The description of this requirement does not refer specifically to the NCP but generally to systems. This requirement therefore encompasses all systems in the end to end process. It is not possible for epSOS to verify systems other than the NCP.

4.2.5.3.2 e1-REQ-5181 Structured Information and Semantic Compliance

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5151 Structured Information and Semantic Compliance

Tested by e1-REQ-4543 Structured Information and Semantic Compliance

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.5.3.3 e1-REQ-5183 Minimum and Maximum Data Sets

Synchronized with e1-REQ-5153 Minimum and Maximum Data Sets

Tested by e1-REQ-5132 Minimum and Maximum Data Sets

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.3.4 e1-REQ-5155 FR08 - Information selection

Tested by e1-REQ-4545 FR08- Information selection

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Deals with the display and selection of prescriptions to the Dispenser and although it cannot be verified by epSOS, it must be verified by a PN HP.

4.2.5.3.5 e1-REQ-5156 FR09 - Prescription presentation

Tested by e1-REQ-4546 FR09- Prescription presentation

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.3.6 e1-REQ-5157 FR10- 'Available' (and thus, valid) prescription

Tested by e1-REQ-4547 FR10- 'Available' (and thus, valid) prescription

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that only prescriptions that are valid are displayed.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.5.3.7 e1-REQ-5158 FR12 - Original prescription

Tested by e1-REQ-4549 FR12- Original prescription

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.3.8 e1-REQ-5159 FR13 - Identification of the medicinal product

Tested by e1-REQ-4550 FR13- Identification of the medicinal product

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

This can be visually validated at the HP-B.

4.2.5.3.9 e1-REQ-5160 FR15 - Dispensed medicine information sent to country A

Tested by e1-REQ-4552 FR15- Dispensed medicine information sent to country A

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Related to e1-REQ-5196 FR14 - Substitution

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.3.10 e1-REQ-5161 FR16 - Univocal relation between original prescription and medicinal product dispensed

Tested by e1-REQ-4553 FR16- Univocal relation between original prescription and medicinal product dispensed

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the data returned to PN A in the eD contains the Prescription Id from the original eP.

4.2.5.3.11 e1-REQ-5162 FR17 - Original dispensed medicine

Tested by e1-REQ-4554 FR17- Original dispensed medicine

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the data returned to PN A in the eD contains the brand name of the Medicinal Product dispensed plus the active ingredient and quantity.

 epSOS <small>EUROPEAN PATIENTS SMART OPEN SERVICES</small>	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
	D5.2.3	Date: 31/01/2013

4.2.5.3.12 e1-REQ-5198 eP is not a collection of patient prescriptions

Tested by e1-REQ-2085 eP is not a collection of patient prescriptions

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.3.13 e1-REQ-5199 REQ 3.3.11 Notification with eDispensation document

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Tested by e1-REQ-4596 REQ 3.3.11 Notification with eDispensation document

Verify that the information passed between two NCPs is structured / converted according to the requirements of epSOS. This has to be verified between the NCPs and further validated visually on the Portal by HP-B.

4.2.5.3.14 e1-REQ-5184 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Synchronized with e1-REQ-5163 Traceability and Exercise of Patient Information Rights

Tested by e1-REQ-4671 Traceability and Exercise of Patient Information Rights

It is assumed that all systems are responsible for auditing data (NCP-A, NCP-B, and Portal). epSOS will verify that all access or attempted access to medical data via the NCP is audited. This is restricted to the NCP-A and NCP-B. epSOS will not verify the traceability of information stored on systems other than the NCP.

4.2.5.3.15 e1-REQ-5186 Data Integrity

Synchronized with e1-REQ-5164 Data Integrity

Tested by e1-REQ-4558 Data Integrity

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Secure communication between NCP's will be verified during interoperability testing. epSOS will verify that the NCP A and B have not damaged, reduced or altered the data in anyway.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.5.3.16 e1-REQ-5188 NFR05 - Access control

Synchronized with e1-REQ-5167 NFR05 - Access control

Tested by e1-REQ-4561 NFR05- Access control

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

epSOS will verify that the NCP is not accessible via any of its interfaces to anyone other than authorised persons. It is not possible for epSOS to verify systems other than the NCP.

4.2.5.3.17 e1-REQ-5189 Data Origin and Data Authenticity

Synchronized with e1-REQ-5168 Data Origin and Data Authenticity

Tested by e1-REQ-4563 Data Origin and Data Authenticity

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Can only be tested between the NCPs.

4.2.5.3.18 e1-FD-261 Features not to be tested

The following features have a functional aspect that do not relate to the functionality between two NCPs, but between an NCP and its respective national infrastructure or its HP. As epSOS does not test the interfaces within the national infrastructures, it is regarded as outside of the scope of this test strategy.

4.2.5.3.19 e1-REQ-5195 FR11 - Access to current prescriptions by dispenser

Tested by e1-REQ-4548 FR11- Access to current prescriptions by dispenser

No centralised test tool will be provided by epSOS, since this is a requirement that is implemented on a voluntary basis. Responsibility to test it is left to the PN piloting it.

4.2.5.3.20 e1-REQ-5197 REQ 3.3.15 eP data are not modifiable by country B

Tested by e1-REQ-4600 REQ 3.3.15 eP data are not modifiable by country B

This is a requirement of a PN. This type of functionality must be restricted to the PN national infrastructure and not the NCP. It must already be standard within a PN national infrastructure as this problem could already occur within their borders.

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

4.2.5.3.21 e1-REQ-5200 REQ 3.3.12 Country A responsibility to update EHR with dispense notification

Tested by e1-REQ-4597 REQ 3.3.12 Country A responsibility to update EHR with dispense notification

This is a requirement of a PN and is implemented on a voluntary basis. Responsibility to test it is left to the PN piloting it.

4.2.5.3.22 e1-REQ-5196 FR14 - Substitution

Tested by e1-REQ-4551 FR14- Substitution

Related to e1-REQ-5160 FR15 - Dispensed medicine information sent to country A

This cannot be tested as it relates solely to a process related to the Dispenser. If a medicine is subsequently substituted, this information must be sent back to Country-A, which is covered in FR15.

4.2.5.3.23 e1-REQ-5185 NFR01 - Service availability

Synchronized with e1-REQ-5169 NFR01 - Service availability

Tested by e1-REQ-4557 NFR01- Service availability

The description relates to operational requirements, the result of which would be the definition of SLA's, and the setting up of a Command Centre responsible for monitoring all systems that are connected directly to the epSOS Infrastructure. It is assumed that epSOS will not create a command centre but allow the PN to regulate themselves.

4.2.5.3.24 e1-REQ-5187 NFR03 - Response time

Synchronized with e1-REQ-5165 NFR03 - Response time

Tested by e1-REQ-4559 NFR03- Response time

The response time of an NCP and the response time between NCPs will be verified to be within the defined parameters. This will be restricted to proving that the roundtrip time between the Portal, NCP-B and NCP-A is not excessively slow. The response time of the PN National Infrastructure will not be measured.

This does not cover the response time of any Country B system other than the NCP, or any

	Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
		Version:	1.0
	D5.2.3	Date:	31/01/2013

other Country A system other than the NCP. However, end-to-end response time will be measured for service evaluation purposes.

4.2.5.3.25 e1-REQ-5190 NFR09 - Trust between countries

Synchronized with e1-REQ-5175 NFR09 - Trust between countries

Tested by e1-REQ-4565 NFR09- Trust between countries

This requirement concerns itself with the non-functional aspect of trust between countries, specifically those policies defined by epSOS and to be implemented by the Participating Nations. The implementation of those policies will be verified through Audits during and post rollout.

4.2.5.3.26 e1-REQ-5192 NFR11 - Single session

Synchronized with e1-REQ-5172 NFR11 - Single session

Tested by e1-REQ-4567 NFR11- Single session

This is a requirement of a PN. This type of functionality must be restricted to the PN national infrastructure and not the NCP. It must already be standard within a PN national infrastructure as this problem could already occur within their borders.

4.2.5.3.27 e1-REQ-5193 NFR12 - Supervision services

Synchronized with e1-REQ-5173 NFR12 - Supervision services

Tested by e1-REQ-4568 NFR12- Supervision services

This concerns operational services and as such is out of scope of epSOS.

These services cover the creation of SLAs and probes, the monitoring of real time performance and services. It is the responsibility of the operational organisations to verify these requirements. This is also coupled with NFR01 – Service Availability.

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.6 e1-FLD-256 Computational Dimension

4.2.6.1 e1-FLD-263 epSOS Test Cases

4.2.6.1.1 e1-TXT-868 Note

The Test Cases are registered directly in the Gazelle test management tool in the Gazelle Master Model.

For more information see D3.C.1 Appendix B #6.1 and <http://gazelle.ihe.net/content/gmm-gazelle-master-model>.

The following actors are defined for the epSOS tests cases:

epSOS Actors
NCP-A - National Contact Point Country A
NCP-B - National Contact Point Country B
CONTENT_CREATOR - Content Creator
CONTENT_CONSUMER - Content Consumer
ARR - Audit Record Repository
SN - Secure Node
TIME_CLIENT - Time Client
TS - Time Server

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.6.1.2 e1-REQ-5210 Pre-Projectathon and PPT-slot Test Cases (Conformance Tests)

Related to e1-REQ-5207 Conformance Test (Pre-Projectathon)

Related to e1-REQ-5209 Pre-Pilot Test

Related to e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

The following are the list of test cases that are used in pre-Projectathons and PPT-slots as of November 2012; i.e. they are the test cases for conformance testing, and need to be completed by individuals against the IHE simulators and validators.

They are available through <http://gazelle.ihe.net/epSOS-doc/> as well.

Code	DisplayName	Description	NCP
epSOS-1	CDA Content Creator	The purpose of this test is to gather sample CDA documents from participating systems	NCP-A and NCP-B
epSOS-2	NCP-A Identification Service	The purpose of this test is to evaluate the capability of the NCP-A to respond to an identification service request	NCP-A
epSOS-3	NCP-A Patient Service	The purpose of this test is to evaluate the capability of the NCP-A to respond to a patient service request. We test here the XCA query	NCP-A
epSOS-4	NCP-A Order Service	The purpose of this test is to evaluate the capability of the NCP-A to respond to an order service request. We test here the XCA query	NCP-A
epSOS-5	NCP-A Dispensation Service	The purpose of this test is evaluate the ability of the NCP-A to receive an eDispensation document from the NCP-B	NCP-A
epSOS-6	NCP-A Consent Service	The purpose of this test is evaluate the ability of the NCP-A to receive an eConsent document from the NCP-B	NCP-A
epSOS-7	NCP-B Identification Service	The purpose of this test is to evaluate the capability of the NCP-B to initiate valid	NCP-B

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

		identification service request	
epSOS-8	NCP-B Patient Service	The purpose of this test is to evaluate the capability of the NCP-B to send a patient service request to the NCP-A. We test here the XCA responses	NCP-B
epSOS-9	NCP-B Order Service	The purpose of this test is to evaluate the capability of the NCP-B to send an order service request to the NCP-A. We test here the XCA responses.	NCP-B
epSOS-10	NCP-B Dispensation Service	The purpose of this test is to evaluate the capability of the NCP-B to send a Dispensation Service Initialize() request to the NCP-A. We test here the XDR document submission	NCP-B
epSOS-11	NCP-B Consent Service	The purpose of this test is to evaluate the capability of the NCP-B to send a consent service request to the NCP-A. We test here the XDR responses	NCP-B

Table - pre-Projectathon and PPT-slot Test Cases

Depending on the services that are implemented by a participant, the following tables show different configurations of conformance test cases:

PN-A Patient Summary	PN-B Patient Summary
epSOS-1	epSOS-1
epSOS-2	epSOS-7
epSOS-3	epSOS-8
epSOS-6	epSOS-11

 Requirement Consolidation II Appendix A	Document Short name:	D5.2.3
	Version:	1.0
D5.2.3	Date:	31/01/2013

PN-A ePrescription	PN-B ePrescription
epSOS-1	epSOS-1
epSOS-2	epSOS-7
epSOS-4	epSOS-9
epSOS-6	epSOS-11
PN-A eDispensation	PN-B eDispensation
epSOS-1	epSOS-1
epSOS-2	epSOS-7
epSOS-5	epSOS-10
epSOS-6	epSOS-11

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

4.2.6.1.3 e1-REQ-5211 Projectathon and PPT-slot Test Cases (Interoperability and Conformance Tests)

Related to e1-REQ-5209 Pre-Pilot Test

Related to e1-REQ-5208 Service Interoperability Test (Projectathon)

Related to e1-REQ-5180 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-5170 Authorized Exchange of Data (»Consent-2«; PIN)

Related to e1-REQ-5186 Data Integrity

Related to e1-REQ-5164 Data Integrity

Related to e1-REQ-5189 Data Origin and Data Authenticity

Related to e1-REQ-5168 Data Origin and Data Authenticity

Related to e1-REQ-5198 eP is not a collection of patient prescriptions

Related to e1-REQ-5155 FR08 - Information selection

Related to e1-REQ-5156 FR09 - Prescription presentation

Related to e1-REQ-5157 FR10- 'Available' (and thus, valid) prescription

Related to e1-REQ-5158 FR12 - Original prescription

Related to e1-REQ-5159 FR13 - Identification of the medicinal product

Related to e1-REQ-5160 FR15 - Dispensed medicine information sent to country A

Related to e1-REQ-5161 FR16 - Univocal relation between original prescription and medicinal product dispensed

Related to e1-REQ-5162 FR17 - Original dispensed medicine

Related to e1-REQ-5154 FR19: Patient Summary of Country A available

Related to e1-REQ-5201 FR21: Patient Summary Conformance

Related to e1-REQ-5202 FR22: Uniqueness of Patient Summary

Related to e1-REQ-5147 HP-B Identification and Authentication

Related to e1-REQ-5176 HP-B Identification and Authentication

Related to e1-REQ-5148 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-5178 L-DP-03 Mutually accepted epSOS agreements on appropriate security measures

Related to e1-REQ-5183 Minimum and Maximum Data Sets

Related to e1-REQ-5153 Minimum and Maximum Data Sets

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Related to e1-REQ-5167 NFR05 - Access control

Related to e1-REQ-5188 NFR05 - Access control

Related to e1-REQ-5149 Patient Identification

Related to e1-REQ-5177 Patient Identification

Related to e1-REQ-5174 Peering Original Document

Related to e1-REQ-5210 Pre-Projectathon and PPT-slot Test Cases (Conformance Tests)

Related to e1-REQ-5199 REQ 3.3.11 Notification with eDispensation document

Related to e1-REQ-5203 REQ 3.3.14 Medication Summary only accessible as part of Patient Summary

Related to e1-REQ-5152 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-5182 Semantic Interoperability of Structured Clinical Content

Related to e1-REQ-5151 Structured Information and Semantic Compliance

Related to e1-REQ-5181 Structured Information and Semantic Compliance

Related to e1-REQ-5163 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-5184 Traceability and Exercise of Patient Information Rights

Related to e1-REQ-5166 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-5194 Willful Disclosure (Data Confidentiality)

Related to e1-REQ-5150 Willful Provisioning of Data (»Consent-1«)

Related to e1-REQ-5179 Willful Provisioning of Data (»Consent-1«)

The following are the list of test cases that are used in Projectathons and PPT-slots as of August 2012; i.e. they are the test cases for mostly interoperability (workflow tests) and partially conformance testing (scrutiny tests), and need to be completed peer-2-peer and by individuals against the IHE validators:

	Requirement Consolidation II Appendix A	Document Short name: D5.2.3
		Version: 1.0
D5.2.3		Date: 31/01/2013

Test-Id	Keyword	Keyword	Version	Status	Peer type
11458	epSOS_Authorization	This test shows the role based access to epSOS documents, according the role description in epSOS Specification	PPT2011	ready	P2P_TEST
11490	epSOS_Scrutiny_Audit_Message	In this test the structure of the Audit Message is verified	PAT2010	ready	NO_PEER_TEST
11562	epSOS_Scrutiny_Certificates	The purpose of this test is to verify the conformity of the certificates with the epSOS requirements.	PPT2011	ready	NO_PEER_TEST
11468	epSOS_Scrutiny_eDispensation	In this test the structure of the CDA L3 document epSOS eDispensation is verified.	PAT2010	ready	NO_PEER_TEST
11479	epSOS_Scrutiny_ePrescription	In this test the structure of the CDA L3 document epSOS ePrescription is verified.	PAT2010	ready	NO_PEER_TEST
11462	epSOS_Scrutiny_PS	In this test the structure of the CDA L3 document epSOS Patient Summary is verified.	PAT2010	ready	NO_PEER_TEST
11563	epSOS_Scrutiny_SAML	The purpose of this test is to verify the conformity of the SAML assertions used in the context of the epSOS project.	PPT2011	ready	NO_PEER_TEST
11472	epSOS_WF_ePresc_eDispens	This test shows the complete workflow in the epSOS ePrescription Service context.	PAT2010	ready	P2P_TEST
11561	epSOS_WF_PS	This test shows the complete workflow in the epSOS Patient Summary Service context.	PPT2011	ready	P2P_TEST

Table - Projectathon and PPT-slot Test Cases

4.2.6.1.4 e1-REQ-5212 Test Cases for end-to-end Functional Testing

Related to e1-REQ-5209 Pre-Pilot Test

Related to e1-REQ-5208 Service Interoperability Test (Projectathon)

End-to-end functional testing is part of both Projectathons and PPT-slots. However, it is not directly managed through the Gazelle® Management Tool, as in the case of the test cases presented in the previous sections. The HPs and/or semantic experts of the participants acting as Country B do several patient data exchanges for both Patient Summary and ePrescription / eDispensation documents, just like the epSOS_WF_PS and epSOS_WF_ePresc_eDispens workflow tests. But instead of technical details, the HPs and/or semantic experts are asked to fill in electronic questionnaires regarding the clinical validity and quality of the exchanged information.

These questionnaires are prepared by epSOS semantic experts, and hosted by IHE-Europe at <http://gazelle.ihe.net/content/epsos-cda-evaluation-form>. The filled in questionnaires are evaluated by epSOS semantic experts. The details of end-to-end functional testing is presented in D3.10.1 Appendix 8 - epSOS end-to-end Functional Testing for Projectathon and Pre Pilot Testing: Guidelines for HPs and PNs.