Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription

epSOS Common Components

WP3.4 Deliverable D3.4.2

< Common Components Specification >

16. July 2010

Document Version: v1.00

Work Package Leader:	**J. Caumanns // FHGISST**
Editing Team:	**J. Caumanns, R. Kuhlisch, O. Rode, S. Bittins // FHGISST**
	S. Lotti, G. Cagnioli // INVITALIA
	M. de Graauw // NICTIZ
	B. Horvat, S. Evdokimov // GEMATIK
	M. Masi, R. Hörbe // ELGA
	Ch. Parisot, K. Witting, B. Majurski // epSOS Industry Team

Content

Document Information

Project name	Smart Open Services – Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription
Author/ person responsible	Jörg Caumanns
Document name	D3.4.2
Status	in process | **submitted to QA** | accepted by QM | approved

History of Alteration

Version	Date	Type of editing	Editorial
0.01	2010-01-14	Organisation	FhG ISST
0.07	2010-03-07	1st draft: ID, Patient, Order, eDisp service	FhG ISST
0.08	2010-03-07	Simplification on eDisp::initialize	FhG ISST
0.09	2010-03-08	2 Flavors: IHE and RLUS (IHE selected for further elaboration by WP3.4)	FhG ISST
0.09IT	2010-03-22	Review of IHE use by Industry Team	Karen, Charles
0.09G	2010-03-22	Chapters 4 and 5 added	FhG ISST
0.20	2010-03-31	Consolidation of 0.09 parts	FhG ISST
0.21	2010-04-07	XCPD and XCA	FhG ISST
0.22	2010-04-09	Full review of chapters 1-3.3; draft for Marc	FhG ISST
0.23	2010-04-13	Finalization of chapter 3. draft for Charles	FhG ISST
0.24	2010-04-15	Finalization of chapter 4/5; integration of new WSDLs and Marc's first review results	FhG ISST
0.25	2010-04-16	QA Release	FhG ISST
0.92	2010-06-04	QA Release (2nd review)	FhG ISST
0.95	2010-06-06	Alignment with WP3.9 and FET	FhG ISST
1.00	2010-07-16	Finalization after comments processing	FhG ISST

Referring Documents

Date	Type	Description	Version	Origin	Document
		epSOS Legal and Regulatory Issues		WP 2.1	[epSOS D2.1.1]
		epSOS ePrescription		WP 3.1	[epSOS D3.1.2]
		epSOS Patient Summary		WP 3.2	[epSOS D3.2.2]
		epSOS Architecture		WP 3.3	[epSOS D3.3.2]
		epSOS Semantic Services		WP 3.5	[epSOS D3.5.2]
		epSOS Identity Services		WP 3.6	[epSOS D3.6.2]
		epSOS Security Services/Policy		WP 3.7	[epSOS D3.7.2]
		epSOS Consolidated Concepts		WP 2.1	[epSOS ConceptPaper]

1 Introduction

The following change history provides an overview of all changes to chapter 1 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

This document is the deliverable D3.4.2 as defined in the annex 1 to the “Smart Open Services for European Patients (epSOS) Large Scale Pilot” contract. It covers the technical specifications of the epSOS common components that have to be put in place by epSOS member states in order to allow for a secure and privacy-aware exchange of identifiable medical data.

1.1 Smart Open Services for European Patients

According to [epSOS Scope], “*the overarching goal of epSOS (Smart Open Services for European Patients) is to develop a practical eHealth framework and ICT infrastructure that will enable secure access to patient health information [...] between European healthcare systems. [...] The methodology will strive to build a common architecture and core services for the identification of users and institutions, security, confidentiality and privacy aspects, and aim to enhance various semantic aspects of the systems.* “

The core principle of epSOS is to bridge existing national eHealth infrastructures instead of setting up a new, centralised European healthcare service network from scratch. To make this approach work technical, semantic and legal interoperability among European eHealth infrastructures must be achieved. This includes identity matters as well as security matters and information management issues within heterogeneous, distributed environments. None of the problems faced by epSOS is new or extremely challenging: cross-border data exchange is common practice in many domains, nearly every European country has use cases and processes for cross-enterprise health data exchange defined and decoupled security services spanning federated domains are well covered by international standards.

Therefore the challenge for the development of technical specifications for the epSOS building blocks is not to find a solution that works for the defined use cases. The challenge is to find a solution that

1) can evolve over the next years and lay ground for a seamless, secure and privacy-aware exchange of any kind of medical data across Europe,
2) can easily connect to the existing infrastructures without imposing unreasonable new risks on the privacy and integrity of existing data managing systems,
3) is flexible enough to be used in conjunction with different means of identification, authentication and authorisation to allow for any citizen and country to participate based on existing legal regulations and technical actualities and
4) is widely accepted and has the potential for reuse of software components and test tools.

The epSOS-II work plan on additional epSOS use cases, more complex data deployment options and patient empowerment services just gives an idea of future requirements that have to be kept in mind.

1.2 epSOS Common Components Specification

The *epSOS Common Components Specification* is the technical baseline of epSOS: There MUST NOT be any normative statement on the shape and behaviour of any epSOS building block that is on a technically lower level than this specification. While specifications on identity management [epSOS D3.6.2] and security services [epSOS D3.7.2] define the core concepts and guidelines for these issues, the *epSOS Common Component Specification* defines the technical means that serve these concepts.

The scope of the *epSOS Common Components Specification* is determined by

- **technical interoperability**: the specification does only cover aspects of cross-border data exchange that are indispensable for technical interoperability
- **shared responsibility:** whenever possible, only the shape of data exchanged “on the wire” is specified while the processes and systems for issuing and consuming these data objects are considered to be national responsibilities

The objective is to define the epSOS interoperability building blocks in a way that they can be implemented independently from each other by different vendors. The *epSOS Common Components Specification* builds upon the implementation independent technology view of [epSOS D3.3.2]. It provides the normative specification of the epSOS services’ operations by mapping them onto established standards.

1.3 Conventions

The keywords MUST, SHOULD, MAY, SHOULD NOT and MUST NOT are used as defined in [RFC 2119].

For indicating the optionality of certain functionalities or data fields the following keywords are used:

- “**R**” or “Required”: Functionalities and data fields marked as “R” MUST be provided.
- The notation “**R+**” is used to indicate that epSOS is stricter on the mandatory nature of the functionality or data field than the underlying base standard.
- “**O**” or “Optional”: Functionalities and data fields marked as “O” MAY be omitted.
- “**R/O**”: Data fields marked as “R/O” are conditionally mandatory.
- “**X**”: Functionalities and data fields marked as “X” MUST NOT be used.

1.4 Organisation of this Document

This document consists of four main parts in order to separate different levels of abstraction and to allow different groups of readers to easily access the information that is relevant for them without having to read the whole document:

- Chapter 2 of this document specifies the functionality of the **epSOS Services** by outlining the data elements that have to be exchanged in order to implement the defined service operations. This epSOS functional service specification is targeted at system architects who are responsible for connecting HCPOs and existing national infrastructures to epSOS components.
- Chapter 3 specifies the implementation of the epSOS services by providing the **epSOS Mappings** of the service operations. These specifications describe how the epSOS services’ operations are mapped onto existing standards and healthcare profiles. This part is targeted at software designers and developers who are responsible for the implementation of epSOS services and for their integration with existing national infrastructure components.
- Chapter 4 defines the **epSOS communication and messaging infrastructure**. It describes the protocols to be used for establishing the epSOS network of trusted nodes and specifies the common formats for messages and audit trail entries. Chapter 4 is mainly targeted at systems administrators who are responsible for the configuration of web service platforms and network nodes.
- Chapter 5 specifies the syntax and semantics of the **assertions and certificates** that are used by the epSOS services. This chapter is targeted at security administrators who are responsible for the management of certificates and the configuration of security services.

Sample messages and the WSDLs for all epSOS services’ interfaces are provided in an appendix to this document.

1.5 Changes from v0.95

The following major changes have been done since version 0.95 of this document:

- both demographic query mode and shared ID query mode are allowed for XCPD
- In order to allow for the integration of additional security safeguards base64 encoded documents MAY be encrypted.

1.6 Open Issues

The following work still has to be done by the editing team:

- ~~verify that the examples are compliant with the schemas that are provided in the appendix (Marc did so for the first one, the others will follow. Therefore: Do NOT comment on schema violations with the examples; we are checking this in parallel to the quality review!).~~
- ~~Some of the WSDLs are still missing (only schemas are provided for the message contents)~~
- ~~two SAML attribute statements (HCPO type, HCP speciality) are not specified. Suggestions for standards to use are welcome...~~
- ~~the tables of references and abbreviations at the end of this document are not complete. They will be updated and completed in parallel with the quality review.~~
- ~~Codes for errors and warnings have not been defined yet. This will as well be done in parallel to the quality review. Therefore: Do NOT comment on missing error codes.~~

2 epSOS Services Functional Specification

The epSOS architecture is based on a service-oriented paradigm. [epSOS D3.3.2] defines the epSOS services and service interfaces and shows how these interact with each other in order to implement the epSOS use cases on patient summary and ePrescription.

This chapter builds upon the technology viewpoint on the epSOS architecture by further refining the functional specification of the epSOS services' interfaces. For each service operation the input and output as well as the requested effect and the preconditions for a success scenario are defined.

2.1 epSOS Service-Oriented Architecture

The following change history provides an overview of all changes to chapter 2.1 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The design of the general architecture of epSOS and the design of the epSOS services is based on the following basic assumptions:

1. The design uses the service-oriented paradigm.
2. All services are passive, the service consumers and service providers communicate synchronously.
3. All epSOS medical data as well as all patient and HCP identity data is administered in autonomous systems. Any exchange of these data is mediated by national gateways following a B2B paradigm.
4. There are no central services except the ones needed for the operation of a secure epSOS infrastructure; the federation of national gateways is implemented via a »circle of trust«.

2.1.1 Service Roles

The service-oriented paradigm distinguishes among three roles: service provider, services consumer, and service registry. The service provider offers a service that is used by the service consumer. The service provider can publish a description of the service in a service registry.

epSOS services are implemented as Web Services whose interfaces are specified with the Web Service Description Language [W3C WSDL 1.1]. epSOS Web services are passive. Communication between services consumer and service provider is always initiated by the service consumer. The service provider is passive and reacts to requests from the service consumer.

The communication between service consumer and services provider is synchronous. The service consumer's control flow is suspended until the service provider has processed the service consumer's request. Service consumer and provider communicate over the Internet using XML-based SOAP messages transported via the HTTP protocol (see chapter 4.3 for details).

Each epSOS service is operated under the responsibility of a National Contact Point (NCP) [epSOS ConceptPaper]. The role of the service consumer is always taken by the NCP of the country of care (country B). The role of the service provider is always taken by the NCP of the country of the patient's affiliation (country A).

A service registry is not used. Instead it is assumed that service descriptions and service location information is made available for service consumers by organisational means and static local directory services (see section 2.1.4). As with other centrally managed data (e. g. value set catalogues and trusted certificates), the mechanisms for securely distributing this information among NCPs are out of the scope of this document and will instead be covered by the epSOS documents on security policies and pilot operations.

2.1.2 Trusted Federation of National Contact Points

National Contact Points (NCPs) are implemented federally in order to allow for a virtual integration of autonomous sources of medical data and identity information [epSOS ConceptPaper]. The independence of the information sources is preserved as all access to an information source is mediated through the epSOS services which are implemented at NCP level. This complies to a Business-to-Business paradigm where end users and data sources are decoupled by enterprise level entry services that map external requests onto internal operations and vice versa. Part of this mediation is the brokerage of trust that is achieved by matching security objects of the NCP-to-NCP trust domain into a local trust domain and vice versa.

The administration of the identities of patients and health care professionals (HCPs) is decentralized. Authentication of a HCP can only be done within the country of care that recognizes this HCP. The existence of a treatment relationship between a patient and a HCP can only be attested within the legal framework of the point of care (PoC). With epSOS HCP authentication and treatment relationship attestment are therefore performed within the country of care (e. g. by using an existing Identity Provider service of the national infrastructure). A brokerage of the HCP authentication and treatment relationship confirmation into the epSOS domain is performed in a way that the NCP at country B confirms the respective claims and maps them onto a unified syntax and semantics that can be processed by the NCP of country A.

The epSOS "Circle of Trust" consists of pairs of mutually trusted consuming and providing gateways. A *consuming gateway* provides the computing environment for the operation of an epSOS service consumer and acts as the exit point from the national domain into the epSOS domain. A *providing gateway* operates the Web Service Endpoint (WSE) of the service provider and acts as the entry point from the epSOS domain into the national domain. Each gateway is operated under the legal responsibility of an NCP.

A basic assumption of epSOS is that mutual trust exists between NCPs. The authenticity and integrity of the services in the gateway-mediated NCP-2-NCP communication is secured with digital certificates. Examinations of the certificates and their exchange (with a limited number of NCPs) are to be synchronized among the epSOS service providers [epSOS D3.7.2, epSOS HLDD].

2.1.3 epSOS Services Overview

To foster interoperability among European healthcare infrastructures without forcing member states to modify their running eHealth services, only NCP gateway-to-gateway interfaces are considered as "normative" with epSOS. These interfaces are provided by web services that use open, XML-based standards and transport protocols to exchange data between gateways.

The full list of epSOS web services acc. to [epSOS D3.3.2] is shown in Table 1.

Service	Mediated Data	Requirements Def.	Functional Spec.	Transaction Spec.
Identification Service	Patient identifiers and demographics	[epSOS D3.6.2]	[epSOS D3.3.2#6.5.1.1] [epSOS D3.4.2#2.2]	[epSOS D3.4.2#3.2]
Patient Service	Patient summary documents	[epSOS D3.2.2]	[epSOS D3.3.2#6.5.1.2] [epSOS D3.4.2#2.3]	[epSOS D3.4.2#3.3]
Order Service	ePrescription documents	[epSOS D3.1.2]	[epSOS D3.3.2#6.5.1.3] [epSOS D3.4.2#2.4]	[epSOS D3.4.2#3.4]
eDispensation Service	eDispensation documents	[epSOS D3.1.2]	[epSOS D3.3.2#6.5.1.4] [epSOS D3.4.2#2.5]	[epSOS D3.4.2#3.5]
Consent Service	Consent documents	[epSOS D3.6.2]	[epSOS D3.3.2#6.5.1.5] [epSOS D3.4.2#2.6]	[epSOS D3.4.2#3.6]

Table 1: epSOS Services Overview

2.1.4 Service Localisation

For the 2011/2012 epSOS pilots service discovery and location will be based on static location tables [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 section 4.4 of this document.

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 of the epSOS technical specifications.[1]

2.1.5 General Considerations for Successful Service Operations

In order to successfully operate the epSOS use cases on patient summary and ePrescription, the following preconditions MUST be met:

1. 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 (see section 4.4). Up-to-date copies of all service providing NCP's Trusted Service Lists MUST be available to the service consumer.
2. A secure channel MUST have been established between service consumer and service provider nodes (see section 4.1 for the establishment of the epSOS Trusted Node Infrastructure).
3. 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 (see section 5.3.5 for the definition of the respective certificate profiles).
4. The requesting HCP MUST have been authenticated in the country of care (see [epSOS D3.6.2] for details on HCP authentication). The service provider MUST be able to verify the attesting HCP identity assertion (see section 5.2 for the specification of the HCP Identity Assertion and section 5.4.7 for the certificate profile of the NCP signature certificate that MUST be used for attesting the successful authentication of an HCP).

Further general requirements for secure and privacy-aware operations that MUST be considered are defined in [epSOS D3.7.2] and [epSOS SecurityPolicy].

2.2 epSOS Identification Service

The following change history provides an overview of all changes to chapter 2.2 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

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 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. 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 (see [epSOS D3.6.2] for further information).

Figure 1 shows the interface of the *epSOS Identification Service* as defined in [epSOS D3.3.2].

[1] 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.

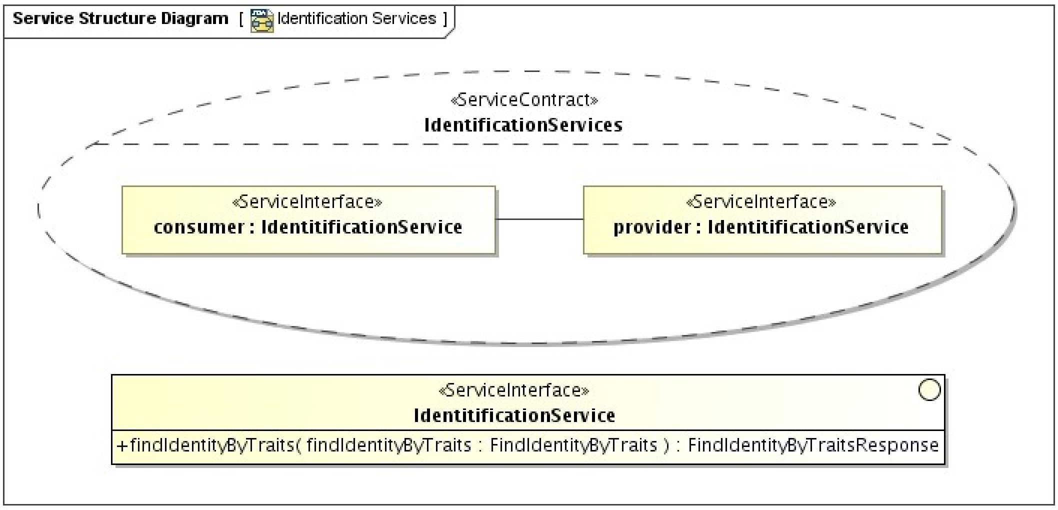

Service Structure Diagram [Identification Services]
«ServiceContract»
IdentificationServices
«ServiceInterface»
consumer : IdentitificationService
«ServiceInterface»
provider : IdentitificationService
«ServiceInterface»
IdentitificationService
+findIdentityByTraits(findIdentityByTraits : FindIdentityByTraits) : FindIdentityByTraitsResponse

Figure 1: epSOS Identification Service Interface

2.2.1 Operation: findIdentityByTraits

Operation	`findIdentityByTraits()`	
Description	Obtain a shared patient identifier	
Requestor	Consuming Gateway at NCP-B (service consumer at the country of care)	
Input Message	FindIdentityByTraitsRequest	
	Body	(1) List of patient identity traits as provided by the patient to the HCP. (2) optional: minimum confidence level that has to be met by the entities that match the provided traits.
	Security Token[2]	[PT] X.509 NCP-B service certificate [ST] 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 HCP 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 section 2.1.5 the following preconditions MUST be met for successful processing: 1. The patient has given a consent that authorises NCP-A to disclose his identity 2. The patient is able to provide identity traits that are sufficient for a unique identification	

[2] PT = Protection Token, ST = Supporting Token (according to [WS SecurityPolicy] definition of security token types)

Main success scenario	Actions of the *epSOS Identification Service* provider: 1. Validate the authenticity of the service consumer 2. Verify HCP identity assertion 3. Verify that the requesting HCP is authorised to query for patient IDs 4. Extract the patient identity traits from the message body 5. Search for patients that match the provided ID attributes 6. 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 - Any other case: throw respective fault 7. 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 HCP 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.

2.3 epSOS Patient Service

The following change history provides an overview of all changes to chapter 2.3 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The *epSOS Patient Service* provides a single operation for retrieving an identified patient’s patient summary from that patient’s country of affiliation.

Figure 2 shows the interface of the *epSOS Patient Service* as defined in [epSOS D3.3.2].

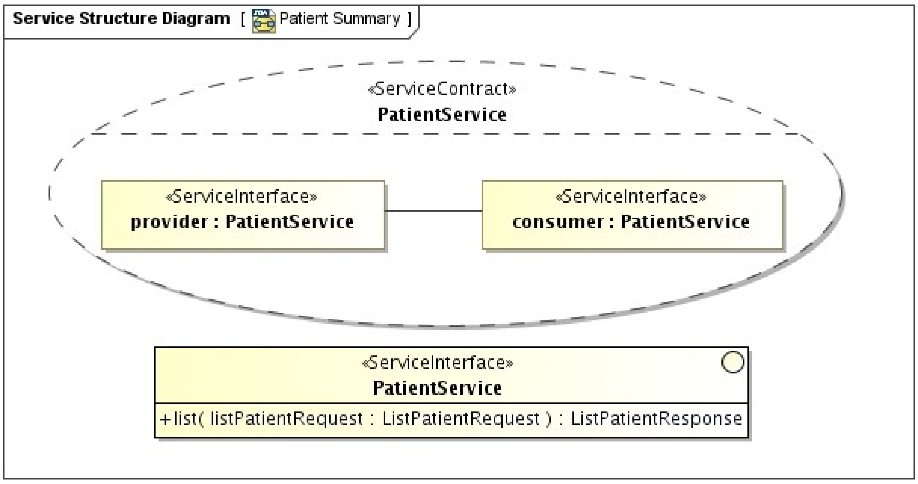

Service Structure Diagram [Patient Summary]
«ServiceContract»
PatientService
«ServiceInterface»
provider : PatientService
«ServiceInterface»
consumer : PatientService
«ServiceInterface»
PatientService
+list(listPatientRequest : ListPatientRequest) : ListPatientResponse

Figure 2: epSOS Patient Service Interface

2.3.1 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 Message	ListPatientRequest	
	Body	(1) Identifier of the patient whose patient summary is requested (2) Optional: epSOS CDA template qualifier (pivot and/or source coded document[3]). 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 [ST] epSOS Treatment Relationship Confirmation Assertion
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	In addition to the requirements stated in section 2.1.5 the following preconditions MUST be met for successful processing: 1. Service consumer and service provider share a common identifier for the patient 2. The patient has given consent to the use of epSOS 3. A valid patient summary for the identified patient is accessible for NCP-A 4. A treatment relationship exists between the patient and the requesting HCP and the attesting assertion can be verified by the service provider 5. The HCP is authorised to access the requested data	
Main success scenario	Actions of the epSOS Patient Service provider: 1. Validate the authenticity of the service consumer 2. Verify HCP identity assertion and TRC assertion 3. Verify that the patient has given valid consent to epSOS and that the consent applies to the current usage scenario 4. Retrieve patient's patient summary source document 5. Enforce national security policy and (if available) patient privacy policy 6. Verify authenticity and integrity of the patient summary 7. Transform patient summary into epSOS pivot format (if requested and needed) and write a respective audit trail entry (see section 4.5.7.3) 8. Render PDF from source document (if requested and needed) 9. Apply epSOS protection means to the response message and send it to the requestor	
Fault Conditions	Preconditions for a success scenario are not met	

[3] In this document the term „source coded document“ is used for an encoding of a medical document that did not undergo any semantic translation. Following [epSOS D3.5.2] it is assumed that PDF/A embedded within CDA is used as the format of choice for source coded documents.

	Requestor has insufficient rights to access the patient's medical summary
	No patient summary is available for the identified patient
	No consent for patient summary sharing is registered for the identified patient
	The patient summary cannot be provided in the requested encoding
	Temporary failure (e. g. verification of preconditions cannot be performed due to a system failure)
Warning Conditions	Country A allows for data hiding; a respective disclaimer SHOULD be shown to the HCP
	The HCP MUST additionally consider the source coded document because this MAY contain additional information
	The computation of the epSOS encoded patient summary was not approved by an HCP; a respective disclaimer MUST be shown to the requesting HCP
	The original data (provided as source coded document) was totally or in parts assembled automatically and has not been approved by a HCP; a respective disclaimer MUST be shown to the requesting HCP

2.4 epSOS Order Service

The following change history provides an overview of all changes to chapter 2.4 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The *epSOS Order Service* provides a single operation for retrieving an identified patient's available ePrescriptions[4] from that patient's country of affiliation.

Figure 3 shows the interface of the *epSOS Order Service* as defined in [epSOS D3.3.2].

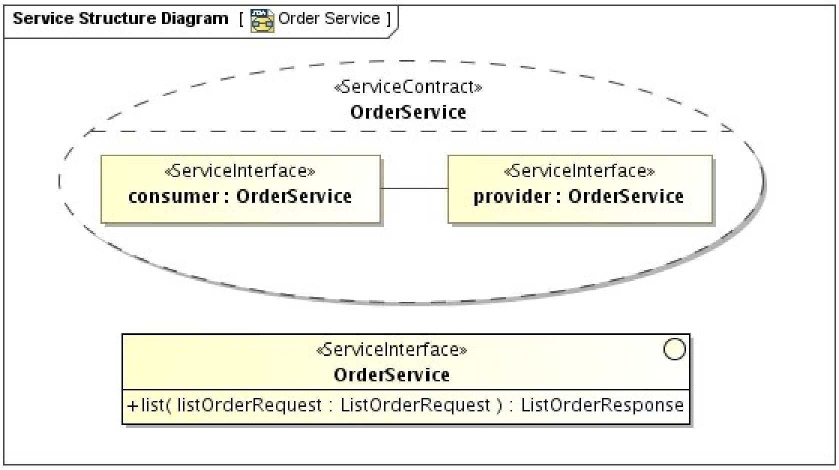


Figure 3: epSOS Order Service Interface

2.4.1 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

[4] For a definition of „available ePrescriptions“ see [epSOS D3.1.2]

	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 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
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 section 2.1.5 the following preconditions MUST be met for successful processing: 1. Service consumer and service provider share a common identifier for the patient 2. The patient has given consent to the use of epSOS 3. A treatment relationship exists between the patient and the requesting HCP and the attesting assertion can be verified by the service provider 4. The HCP is authorised to access the requested data	
Main success scenario	Actions of the epSOS Order Service provider: 1. Validate the authenticity of the service consumer 2. Verify HCP identity assertion and TRC assertion 3. Verify that the patient has given valid consent to epSOS and that the consent applies to the current usage scenario 4. Retrieve patient’s available prescriptions source documents 5. Enforce national security policy and (if available) patient privacy policy 6. Verify authenticity and integrity of available prescriptions 7. Transform ePrescriptions into epSOS pivot format (if requested and needed) and write a respective audit trail entry (see section 4.5.7.3) 8. Render PDF from source document (if requested and needed) 9. Apply epSOS protection means to the response message and send it to the requestor	
Fault Conditions	Preconditions for a success scenario are not met	
	Requestor has insufficient rights to access the patient’s ePrescriptions	
	No consent for ePrescription sharing is registered for the identified patient	
	A (referenced) ePrescription cannot be provided in the requested encoding	
	Temporary failure (e. g. authenticity verification cannot be performed due to a PKI failure)	
Warning Conditions	Country A allows for data hiding; a respective disclaimer SHOULD be shown to the HCP	
	Country A legislation assigns the task of checking for contraindications and drug interaction to the dispenser. A warning MUST be shown to the HCP in country B that the checks for contraindication and drug interaction MAY not have been performed on the prescribed medication in country A.	
	Mandatory fields have been nullified for some of the provided ePrescriptions (minimum dataset is not fully provided[5]); the HCP MUST additionally 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 HCP; a respective disclaimer MUST be shown to the HCP	
	A (referenced) ePrescription is time valid for dispensation but not for reimbursement. A message SHOULD be shown to the HCP that he SHOULD inform the patient that his health insurance will not reimburse the dispensed medicine.	

2.5 epSOS Dispensation Service

The following change history provides an overview of all changes to chapter 2.5 that have been done since v1.00 of this document.

[5] 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 *epSOS Dispensation Service* provides an operation for notifying the patient's country of affiliation on the dispensation of a previously retrieved ePrescription. As dispensation information MAY be used by a country to automatically update internal patient data (e. g. list of current medication) an additional operation is provided to roll back the effects of a dispensation notification (e.g. in case of an error or if the patient rejects the medication after the dispensation notification has been sent)[6].

Figure 4 shows the interface of the *epSOS Dispensation Service* as defined in [epSOS D3.3.2].

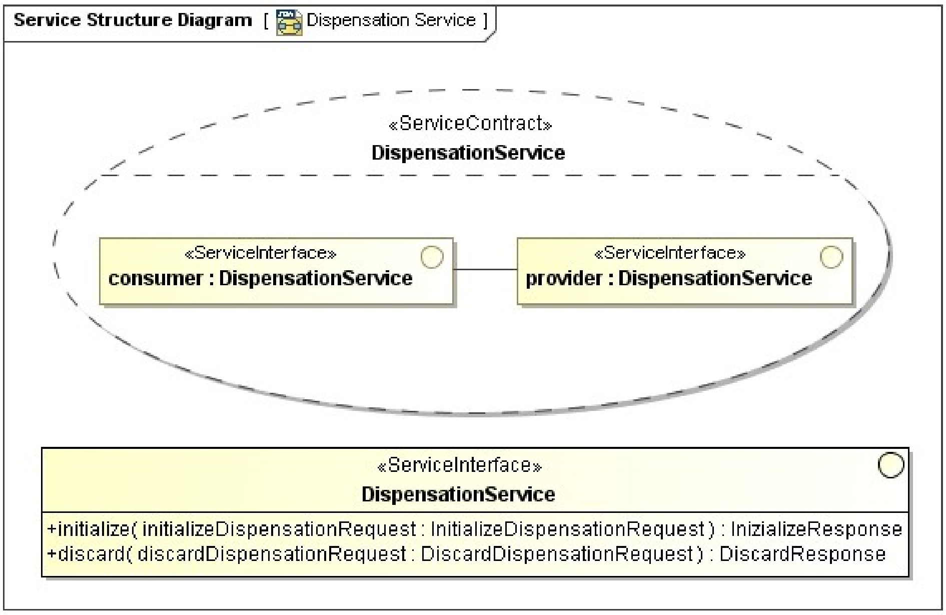

Service Structure Diagram [Dispensation Service]
«ServiceContract»
DispensationService
«ServiceInterface»
consumer : DispensationService
«ServiceInterface»
provider : DispensationService
«ServiceInterface»
DispensationService
+initialize(initializeDispensationRequest : InitializeDispensationRequest) : InizializeResponse
+discard(discardDispensationRequest : DiscardDispensationRequest) : DiscardResponse

Figure 4: epSOS Dispensation Service Interface

2.5.1 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	initializeDispensationRequest	
	Body	(1) epSOS coded eDispensation documents as defined by [epSOS D3.5.2]. (2) source coded dispensation data 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 epSOS coded eDispensation documents.
	Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion
Output Message	initializeDispensationResponse	

[6] The respective discard( ) operation is introduced in [epSOS 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 [epSOS D3.1.2].

in successful Case	Body	(1) Success indicator
	Security Token	[PT] X.509 NCP-A service certificate
Precondition of success scenario	In addition to the requirements stated in section 2.1.5 the following preconditions MUST be met for successful processing: 1. Service consumer and service provider share a common identifier for the patient 2. The patient has given consent to the use of epSOS 3. The service consumer has previously retrieved the list of the patient's available ePrescriptions 4. All available ePrescriptions for the identified patient are accessible for NCP-A and the provided eDispensation data relates to these ePrescriptions 5. A treatment relationship exists between the patient and the requesting HCP and the attesting assertion can be verified by the service provider 6. The HCP is authorised to dispense medication for the patient	
Main success scenario	Actions of the epSOS Dispensation Service provider: 1. Validate the authenticity of the service consumer 2. Verify HCP identity assertion and TRC assertion 3. Verify that the patient has given consent to epSOS and that the consent is valid 4. Enforce national security policy and (if available) patient privacy policy 5. Verifiy that all dispensation information is provided and that dispensation data is properly coded 6. Retrieve patient's available prescriptions and verify that each dispensation item matches with a prescribed item 7. Process the dispensation information 8. Apply epSOS security measures to the success indicator and send it to the requestor	
Fault Conditions	Preconditions for a success scenario are not met	
	The requesting HCP has insufficient rights to dispense the identified patient's ePrescriptions	
	One or more of the provided dispensation items do not relate to available ePrescriptions of the identified patient	
	The ePrescription that is referred to by an eDispensation has already been dispensed.	
	No consent for ePrescription sharing and dispensing is registered for the identified patient	
	The eDispensation data is not provided in all mandatory encodings	
	Temporary failure (e.g. verification of a signature cannot be performed due to a PKI failure)	
Warning Conditions	eDispensation data is not processed by the patient's country of affiliation	

2.5.2 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 section 2.1.5 the following preconditions MUST be met for successful processing: 1. Service consumer and service provider share a common identifier for the patient 2. The service consumer has previously retrieved the list of the patient's available ePrescriptions and dispensed the identified medicine	

Main success scenario	Actions of the epSOS Dispensation Service provider: 1. Validate the authenticity of the service consumer 2. Verify HCP identity assertion 3. Extract the dispensed item id from the message body and ensure that this item was previously dispensed by the identified HCP 4. Enforce national security policy and (if available) patient privacy policy 5. Rewind the dispensation 6. Sign the success notification and send it to the requestor
Fault Conditions	Preconditions for a success scenario are not met
	The HCP has insufficient rights to process the patient's ePrescription data
	The HCP was not the original dispenser of the identified medication item
	The identified item had not been dispensed previously
	Temporary failure (e.g. service provider is temporarily unable to access an internal service)
Warning Conditions	eDispensation data is not processed by the country of affiliation
	eDispensations are not rolled back automatically by the country of affiliation

2.6 Consent Service

The following change history provides an overview of all changes to chapter 2.6 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The epSOS consent service provides operations for the remote management of consents (e. g. giving and revoking consent from abroad). Figure 5 shows the interface of the epSOS patient service as defined in [epSOS D3.3.2].

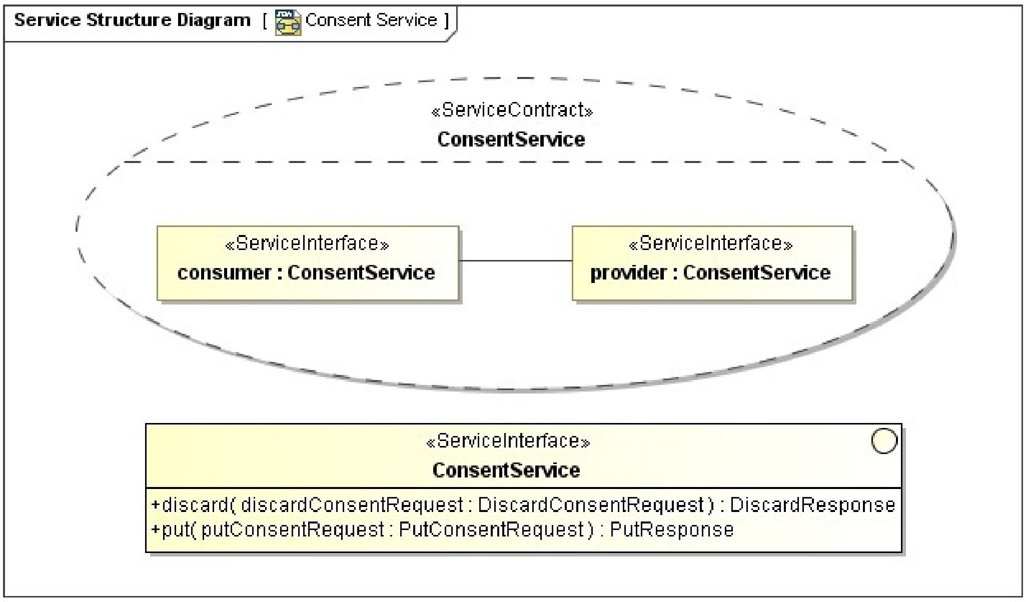

Service Structure Diagram [Consent Service]
«ServiceContract»
ConsentService
«ServiceInterface»
consumer : ConsentService
«ServiceInterface»
provider : ConsentService
«ServiceInterface»
ConsentService
+discard(discardConsentRequest : DiscardConsentRequest) : DiscardResponse
+put(putConsentRequest : PutConsentRequest) : PutResponse

Figure 5: epSOS Consent Service Interface

2.6.1 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 Message	putConsentRequest	
	Body	(1) Information on the newly given or revoked consent (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
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 section 2.1.5 the following preconditions MUST be met for successful processing: 1. Service consumer and service provider share a common identifier for the patient 2. The patient has confirmed in the consent status change	
Main success scenario	Actions of the epSOS Consent Service provider: 1. Validate the authenticity of the service consumer 2. Verify HCP identity assertion 3. Verify that the requested status change is allowed by country-A security policies 4. Apply the consent status change for the country of care 5. 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[7] (e.g. by signing the consent document)	
	Country-A legislation requires that a scanned consent document is provided with the request[8]	
	Temporary failure (e.g. service provider is temporarily unable to access an internal service)	
Warning Conditions	Consent status change requests are not processed by the country of affiliation	
	Consent status changes are not applied automatically by the country of affiliation. Therefore the consent status change will not be immediately operative.	

2.6.2 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
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 section 2.1.5 the following preconditions MUST be met for successful processing: 1. The service consumer has previously triggered a consent change and is responsible for the consent document that is to be discarded	

[7] It is assumed that the member state 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 stataus changes from abroad (The alternative would have been a static configuration or a dedicated operation for querying a country’s consent policy).,

[8] see previous footnote

Main success scenario	Actions of the epSOS Consent Service provider: 1. Validate the authenticity of the service consumer 2. Verify HCP identity assertion 3. Extract the consent document id from the message body and ensure that this consent status change was previously triggered by the identified HCP 4. Enforce national security policy and (if available) patient privacy policy 5. Trigger the roll back of the consent giving/revocation 6. Sign the success notification and send it to the requestor
Fault Conditions	Preconditions for a success scenario are not met
	Country-A legislation does not allow for discarding a consent; a new consent is required
	The HCP was not the original mediator of the identified consent document
	The identified document is not known
	Temporary failure (e.g. service provider is temporarily unable to access an internal service)
Warning Conditions	Consent status change requests are not processed by the country of affiliation
	Consent status changes are not rolled back automatically by the country of affiliation

3 epSOS Service Implementation

The epSOS service interface defines the semantics of identification and data sharing operations for European health services. “On the wire” the service operations are implemented by SOAP messages that are exchanged between an initiating gateway (operated by NCP-B) and a providing gateway (operated by NCP-A).

This chapter specifies the mapping of epSOS service operations onto standardised messages and as such is the normative implementation guideline for the epSOS-facing NCP interface.

3.1 Conventions and Restrictions

The following change history provides an overview of all changes to chapter 3.1 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

3.1.1 NCP: A Standards based Implementation

The epSOS NCP-2-NCP interface is based on the IHE X* family of Interoperability Profiles (Figure 6)

Figure 6: IHE actors and transactions that are profiled by epSOS

The IHE profiles that lay ground for epSOS NCP-to-NCP data exchange are:

- Cross-Community Access (XCA)
- Cross-Enterprise Document Reliable Interchange (XDR)
- Cross-Community Patient Discovery (XCPD)

The epSOS service specifications that build on these IHE profiles introduce various extensions and restrictions on IHE actor and transaction definitions in order to properly cover the epSOS use cases and to align with the epSOS security framework:

- Registry query and repository retrive transactions are conflated to a single list() operation (see section 3.1.2).
- Additional error messages are defined that cover specific failure conditions of the epSOS use cases on patient summary and ePrescription.

- Warning messages are introduced (see section 3.1.4) to allow for notifications on specific environmental conditions that apply to a member state and that MAY affect the interpretation of data in another member state.
- The optionality of data fields is aligned to European privacy regulations.
- The application of security measures and the contents of the SOAP security header are specified normatively (see section 4.3.5)

3.1.2 IHE XCA Extension: LeafClassWithRepositoryItem Response Format

IHE XCA defines message interchange formats for listing and retrieving patient related documents. It is based on a stored query model[9] where the requestor provides attribute-value pairs in the query. It is up to the responding site to map the query attributes onto its internal registry information model. For documents matching the provided attributes' values, the document identifiers (and minimum metadata) are provided. The initiator of the original request may then chose a subset of these listed documents to issue a simple retrieve based on the document identifiers.

At this point IHE XCA only supports scenarios where a query to request a list is first performed by returning document metadata (»LeafClass«) or just document IDs (»ObjectRef«), followed by a document retrieve operation.

In contrast epSOS is based on a pattern, that allows for easier handling of dynamic data and keeps the NCP-A stateless [epSOS D3.3.2]. For epSOS the retrieval of a single patient summary or a patient's set of ePrescriptions is performed by a single list() operation which returns all objects that match a given filter query within the response message. In order to implement this epSOS document sharing pattern, epSOS introduces a new "LeafClassWithRepositoryItem" format for returning documents on otherwise XCA compliant queries. This epSOS defined XCA option allows for an integrated query and retrieve message (see Figure 7).

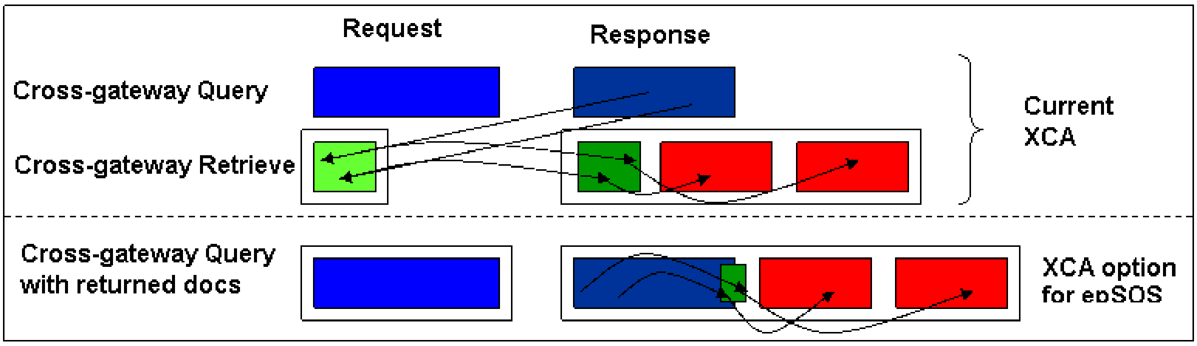


Figure 7: epSOS list() operation with metadata (dark blue), XOP reference (green) and attached documents (red)

The *Cross-Gateway Query With Returned Documents* extension is a combination of the *Cross Community Query Response* and the *Cross Community Retrieve Response* messages. The pure XML of the response message introduces a new XML element `<Document/>` with namespace urn:ihe:iti:xds-ebrim:extensions:2010. This element may appear as the last element child of an `<ExtrinsicObject/>` element. It may appear zero or one times. This element contains the base64-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 message. This format is considered the unoptimized format - the only one that can be represented in pure XML. This is not the wire-format for the message but is what is specified by the schema and the WSDL (the XOP/MTOM optimization is applied afterwards).

The respective part of the `<DocumentEntry/>` metadata looks like this:

[9] IHE XCA – as IHE XDS.b – does not exchange full query statements but only query arguments that are filled into predefined slots of a database stored query at the service side.

```
<rim:ExtrinsicObject>
  <!-- lots of stuff missing here -->
  <xdsext:Document xmlns:xdsext="urn:ihe:iti:xds-ebrim:extensions:2010">
            VGhpcyBpcyBteSBkb2N1bWVudC4KCkl0IGlzIGdyZWF0IQo=
  </xdsext:Document>
</rim:ExtrinsicObject>
```

The MTOM/XOP optimization of this content replaces the contents of the `<Document/>` element with a XOP reference to a different MIME part which holds the content[10]. It is this moving of the bulky content out of the XML where it is difficult to handle and into the raw MIME multipart frame that is considered the optimization of MTOM/XOP. The resulting <Document/> element looks like:

```
<xdsext:Document xmlns:xdsext="urn:ihe:iti:xds-ebrim:extensions:2010">
  <xop:Include href="cid:1.urn:uuid:F862C3E04D9E35266C1256303956117@apache.org"
             xmlns:xop="http://www.w3.org/2004/08/xop/include"/>
</xdsext:Document>
```

The `@href` attribute is the Content-ID of the MIME Part holding the actual contents. This Content-ID becomes a pointer to the contents of the document.

The query request message XML is syntactically identical to that of IHE Cross Community Query request with two extensions:.

- The `<ws:Action/>` is “urn:ihe:iti:2010:CrossGatewayQueryRetrieve”
- Inside the `@AdhocQueryRequest/ResponseOption`, the returnType “LeafClassWith-RepositoryItem” MUST be used. This value, specified by ebRS version 3.0, indicates that both the full metadata plus the document contents are to be returned.

3.1.3 Error Handling

Failures during operation execution can be of different kinds; e. g. they may be caused by syntactic mismatches, insufficient access rights or country-A component failures. epSOS makes use of three different error reporting mechanisms in order to allow for a better handling of errors on the appropriate level of abstraction (see Figure 8):

- SOAP faults: The standard SOAP fault mechanism is used for failures that originate in the encoding of the SOAP message or the contents of the SOAP header. 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.
- Error Messages in the SOAP response body: Error reporting mechanisms of the business level protocol (e. g. XCA) are 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. The failure usually either originates at the Point of Care in country B or at the national infrastructure in country A. These errors SHOULD be reported to the HCP in country B as it is assumed that either the HCP or the patient MAY be able to take action to successfully re-issue the request. Typical examples of such errors are missing consents and temporary component failures in country A.
- 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

[10] It must be noted that the ebRS v3.0 standard does not support MTOM/XOP. Therefore the required epSOS extension to the IHE XCA profile even affects the implementation of the underlying OASIS ebXML standard. Nevertheless MTOM/XOP support for ebRS will be part of the forthcoming version 4.0.

elements of clinical information missing (e.g. in a patient summary). These clinical content errors should be conveyed within the document content. The SOAP body transactions and SOAP header were exchanged without errors at the lower two levels.

Figure 8: epSOS error handling

A list of all SOAP fault codes and conventions to be followed for transmitting SOAP faults are provided in section 4.6 of this document. Business level error messages and their proposed processing are provided in the "response message" sections of the epSOS service specifications.

3.1.4 Information Messages and Warnings

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 HCP in the country of care. An example for this is a notice on automatically collected data that was not approved by an HCP. 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 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 are reported in an explicit clinical statement within that document.

3.1.5 Object Identifier

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
1.3.6.1.4.1.12559.11.10.1.3.2.1	Patient Identification related codes and code systems
1.3.6.1.4.1.12559.11.10.1.3.2.2	HCP(O) identification, authenication, 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 a full list of all WP3.4 defined OIDs see appendix 6.2.2 of this document.

3.1.6 Namespaces

XML namespace prefixes are used in this document to stand for their respective namespaces as follows:

Prefix	Namespace
epsos	urn:epsos:v1
soapenv	http://www.w3.org/2003/05/soap-envelope
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
rimext	urn:ihe:iti:xds-ebrim:extensions:2010[11]
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#

3.2 epSOS Identification Service

The following change history provides an overview of all changes to chapter 3.2 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The *epSOS Identification Service* is 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.

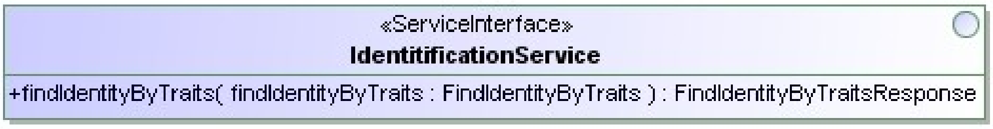

«ServiceInterface»
IdentitificationService
+findIdentityByTraits(findIdentityByTraits : FindIdentityByTraits) : FindIdentityByTraitsResponse

Figure 9 - Patient Identification Service Interface

The implementation of the *epSOS Identification Service* is based on the standard

- HL7 IS: HL7 V3 Identification Service

and is an extension to the IHE profile

- XCPD: IHE Cross-Community Patient Discovery [IHE XCPD]

3.2.1 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] transactions.

3.2.1.1 Request Message

The *findEntityByTraits()* request is initiated by an HCP 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].

[11] IHE will be asked to block this namespace for epSOS extensions in order to avoid conflicts with forthcoming IHE extensions to the ebRIM.

For the HL7 transmission wrapper and the *HL7 Control Act* the conventions identified in the IHE PIX/PDQV3 supplement appendix O [IHE PIX/PDQv3] and the changes from the XCPD supplement appendix O MUST be followed.

In addition the following epSOS-specific restrictions apply:

- <receiver/> 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. <sender/> 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 [epSOS 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] MUST NOT be used.
- The *health data locator option* as defined in section 27.2.1 of [IHE XCPD] 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] 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] MUST NOT be used.
- 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.

3.2.1.2 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 <LivingSubject-ID/> element.
LivingSubjectName	Personal ID Card	Family name and given name MUST both be given
LivingSubjectBirthTime	Personal ID Card	MUST be encoded as “yyyymmdd”
LivingSubjectGender		MUST be “M” or “F”
LivingSubjectBirthPlaceAddress	Personal ID Card	SHOULD contain country and city.
patientAddress	Personal ID Card	SHOULD contain country and city.

For detailed information on the encoding of these traits and their optionality for the XCPD modes see [IHE XCPD].

3.2.1.3 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 HCP in country B to verify the accuracy of the identification.

3.2.1.4 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 services. 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 identifer 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 identifer and authentication object by their roots (assigning authorities).

3.2.1.5 Requested Accuracy of Matches

The *HL7 Patient Registry Find Candidates Query* allows to further refine the match criteria by setting the match algorithm and specifying a requested minimum degree of match for the provided traits.

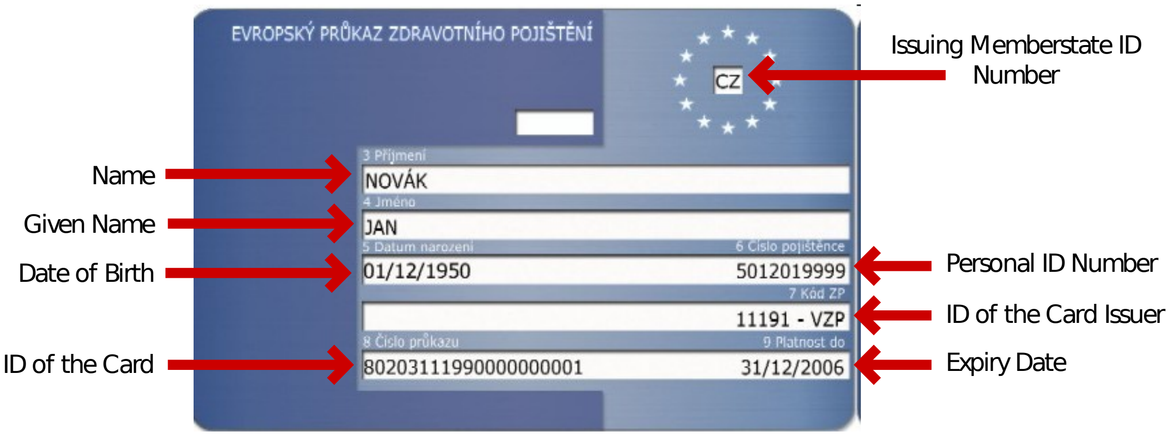
As the respective <MatchCriterionList> element is optional with the HL7 schema, it SHOULD NOT be used for the epSOS pilots. If present, the minimum requested match degree SHOULD be set to an integer value of “100”. In both cases the responding service SHOULD only respond with identity data of patients who fully match all provided traits.

3.2.1.6 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="...">
    <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>
  </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="80203111990000000001"/>
                    <hl7v3:semanticsText/>
                </hl7v3:livingSubjectId>
                <hl7v3:livingSubjectName>
                    <hl7v3:value>
                        <hl7v3:family>NOVAK</hl7v3:family>
                        <hl7v3:given>JAN</hl7v3:given>
                    </hl7v3:value>
                    <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>
```

3.2.1.7 Expected Actions

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[12].

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 section 4.6 of this document.

3.2.1.8 Response Message (Full Success Scenario)

The *epSOS findEntityByTraits response* content is based on *HL7 Patient Registry Find Candidates Query Response (PRPA_IN201306UV02)* interaction, as profiled by the *IHE XCPD Cross-Gateway Patient Discovery* 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:

- <receiver/> 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. <sender/> 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 [epSOS 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] MUST NOT be used.

[12] The national security policy of the patient's country of affiliation always overrides service consumer minimum confidence level: for instance, if country A only accept 100% match but country B is requesting with minimum confidence level of 75%, then only 100% matches will be returned (see [epSOS D3.6.2] for details on ID traits matching and confidence levels).

- The <processingCode/> 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 <subject/> element MUST be included within the control act wrapper.

In addition to the constraints defined in [IHE XCPD] the following conventions MUST be followed for <subject1/patient/> elements:

Element Name	Opt.	epSOS Usage Convention
`Patient`	R	For each matching candidate a single <patient/> 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 patent’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]. 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:
		`<hl7v3:queryMatchObservation classCode="OBS" moodCode="EVN">`
		`  <hl7v3:code codeSystem="2.16.840.1.113883.1.11.19914"/>`
		`  <hl7v3:value xsi:type="hl7v3:INT" value="MATCH"/>`
		`</hl7v3:queryMatchObservation>`

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 <patientPerson /> 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 HCP 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 with the response.
birthTime	R+	MUST be provided as “yyyymmdd”
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], 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)

3.2.1.9 Response Message (No Patient ID Discovered)

If the *epSOS Identification Service* provider does not find a matching patient identifier it MUST 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>
```

Depending on the reason for not providing a patient identifier, the codes and messages as defined below MUST be used[13]:

Condition and proposed action	Reason Encoding

The service requestor tried an identification based on an ID only or did not provide enough data to univocally identify the patient. (WARNING)
The HCP SHOULD ask the patient for further demographics and re-issue the request.
AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper).
OK (data found, no errors) is returned in QueryAck.queryResponseCode (control act wrapper)
	`<triggerFor typeCode="TRIG">`
	`  <actOrderRequired classCode="ACT" moodCode="RQO">`
	`    <code code="AdditionalDemographicsRequested"`
	`          codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/>`
	`  </actOrderRequired>`
	`</triggerFor>`
	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.

The service provider only allows for patient identification by national/shared ID (WARNING).
The HCP SHOULD ask the patient for a national (health care) identification card and re-issue the request using *Shared/national Patient Identifier Query and Feed mode.*
AA (application accept) is returned in Acknowledgement.typeCode (transmission wrapper).
AE (application error) is returned in QueryAck.queryResponseCode (control act wrapper)
	`<triggerFor typeCode="TRIG">`
	`  <actOrderRequired classCode="ACT" moodCode="RQO">`
	`    <code code="DemographicsQueryNotAllowed"`
	`          codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/>`
	`  </actOrderRequired>`
	`</triggerFor>`

The service provider only allows for patient identification by national health card or EHIC. Queries based on demographics only are not supported (WARNING)
The HCP SHOULD ask the patient for a health care identification card and 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)
	`<triggerFor typeCode="TRIG">`
	`  <actOrderRequired classCode="ACT" moodCode="RQO">`
	`    <code code="EHICDataRequested"`
	`          codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/>`
	`  </actOrderRequired>`
	`</triggerFor>`

The service provider does not accept the query because responding MAY lead to a	`<mitigatedBy typeCode="MITGT">`
	`  <DetectedIssueManagement`
	`        classCode="ACT" moodCode="RQO">`

[13] 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.

disclosure of private patient data (ERROR). The HCP SHOULD limit the provided traits and 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="PrivacyViolation" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </DetectedIssueManagement> </mitigatedBy>
The requestor has insufficient rights to query for patient's identity data (ERROR). If access to the patient's medical data is required at the PoC this MUST be performed by a person with additional permissions. 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="RQO"> <code code="InsufficientRights" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </DetectedIssueManagement> </mitigatedBy>
Patient authentication MUST be piggybacked with patient identification. A respective identifier (e.g. GSS TAN) was not provided (ERROR) The HCP 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)	<mitigatedBy typeCode="MITGT"> <DetectedIssueManagement classCode="ACT" moodCode="RQO"> <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="RQO"> <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="RQO"> <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="RQO"> <code code="PolicyViolation"

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>`

3.2.1.10 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">
        <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>
  </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="RQO">
                        <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>
        </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>
```

3.2.2 Security Audit Considerations

Both the *epSOS Identification Service* provider and consumer write an audit trail entry according to the ID Mapping audit schema as defined in section 4.5.5. 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	HCP 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

Table 2: epSOS Patient Identification Service Audit Message Categories

3.2.3 Protocol Requirements

The *epSOS Patient Identification Service* FindIdentityByTraits request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in section 4.3 of this document.

Port types and bindings MUST be used as defined in the WSDL given in section 6.4.1 of this document. Acc. to this the epSOS FindIdentityByTraits operation's request and response data MUST be contained within the message body as follows:

epSOS Patient Identification Service	Message Body
FindIdentityByTraits request	PRPA_IN201305UV02_Message (see section 6.4.1)
FindIdentityByTraits response	PRPA_IN201306UV02_Message (see section 6.4.1)

The request message MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document. The response message MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document.

3.3 epSOS Patient Service

The following change history provides an overview of all changes to chapter 3.3 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The *epSOS Patient Service* is 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.

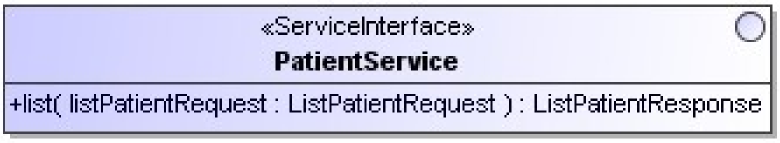

«ServiceInterface»
PatientService
+list(listPatientRequest : ListPatientRequest) : ListPatientResponse

Figure 10 - Patient Service Interface

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[14] [OASIS ebRS 3.0]
- MTOM: SOAP Message Transmission Optimization Mechanism [W3C MTOM]
- XOP: XML-binary Optimized Packaging [W3C XOP]

and is an extension to the IHE profile:

- XCA: IHE Cross-Community Access [IHE XCA]

For discovery and localisation of the Patient Service instance that is responsible for providing access to the identified patient's data see section 2.1.4 of this document.

3.3.1 List() Operation

The *epSOS Patient Service* list() operation is implemented as an extension to the IHE XCA Cross-Gateway Query 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 Retrieve (SOAP 1.2 MTOP with XOP encoding attachments).

[14] 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.

3.3.1.1 Request Message

The list() request is initiated by an HCP in the country of care for retrieving the patient summary of an identified patient. The respective request message builds upon the IHE XCA Cross-Gateway Query request message.

The <AdhocQueryRequest/> element that encapsulates the query parameters MUST be used as follows for epSOS:

Element Name	epSOS Usage Convention
`ResponseOption/@returnComposedObjects`	MUST be “true” (per XCA).
`ResponseOption/@returnType`	MUST be “LeafClassWithRepositoryItem” (per epSOS extension, see section 3.1.2)
`AdhocQuery`	Container for holding the ebML stored query arguments. All arguments MUST be encoded as query slots (see table below).
`AdhocQuery@id`	MUST use the Find Documents query ID from Cross-Gateway Query transaction (XCA-ITI-38): "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d"

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.

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:ResponseStatusType:Approved'
`$XDSDocumentEntryClassCode`	R	Patient summary LOINC code ("34133-9") coded according to specification in ITI TF-2a: 3.18.4.1.2.3.4 Coding of Code/Code-Scheme. As classification scheme 2.16.840.1.113883.6.1 MUST be used: `'34133-9^^2.16.840.1.113883.6.1'`
`$XDSDocumentEntryTypeCode`	O	Patient summary LOINC code ("34133-9") 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: `'34133-9^^2.16.840.1.113883.6.1'`
`$XDSDocumentEntryFormatCode`	O	Format qualifier as defined in table 1C of [epSOS D3.5.2C]; see table below for details on applying these codes to the retrieval of a patient’s medical summary. Only encodings of the patient summary that comply to the requested format code will be returend by the service provider. If this stored query slot is omitted the service provider MUST deliver all available encodings[15].
`$IncludeAssociations`	O	If used, MUST be ‘yes’. SHOULD be omitted if only a single encoding is requested.

For the document format only the format codes defined in [epSOS D3.5.2C] and listed in the following table MUST be used.

[15] 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.

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 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-enveloped 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.

3.3.1.2 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 43133-9) of an identified patient (patient identifier 90378912821). In this example the service consumer does not specify the requested encoding. Therefore the service provider MUST deliver all available encodings (e. g. epSOS pivot and source coded document).

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" ... >
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
   <rim:AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
      <rim:Slot name="$XDSDocumentEntryPatientId">
         <rim:ValueList>
            <rim:Value>'90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO'
            </rim:Value>
         </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="$XDSDocumentEntryStatus">
         <rim:ValueList>
            <rim:Value>('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')
            </rim:Value>
         </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="$XDSDocumentEntryClassCode">
         <rim:ValueList>
            <rim:Value>('34133-9^^2.16.840.1.113883.6.1')</rim:Value>
         </rim:ValueList>
      </rim:Slot>
      <!-- Include associations whose sourceObject and targeObject attributes
           reference ExtrinsicObjects returned -->
      <rim:Slot name="$IncludeAssociations">
         <rim:ValueList>
            <rim:Value>'yes'</rim:Value>
         </rim:ValueList>
      </rim:Slot>
   </rim:AdhocQuery>
</soapenv:Body>
</soapenv:Envelope>
```

3.3.1.3 Expected Actions

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, see section 3.3.1.4) or
- an error message (no patient summary provided, see section 3.3.1.5).

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 section 4.6 of this document.

3.3.1.4 Response Message (Full Success Scenario)

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 XCA Cross-Gateway Query response and Cross-Gateway Retrieve Response messages, by creating a new combined QueryRetrieve message[16].

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 XCA Cross-Gateway Stored Query response message [IHE XCA]
`@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" (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].
`../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 Table 3 below.
`../../../rimext:Document`	This is an epSOS specific extension to [IHE XCA]. 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] MUST be used. If no restrictions on metadata values are given, the metadata elements MUST be used as per [IHE XCA].

Metadata (ebRIM names)	Binding	epSOS Opt.	epSOS usage convention

[16] A respective change request to include this extension with the IHE XCA profile has been agreed with the profile authors and proposed to IHE ITI Technical Committee.

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 “yyyymmdd”
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.
repositoryUniqueId	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.
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.
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 ("34133-9"). 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 XCA compatibility but MAY be ignored by the service consumer. Value SHOULD be set to “Not Used”.
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 XCA compatibility but MAY be ignored by the service consumer. Value SHOULD be set to “Not Used”..
practiceSettingCode	Classification	R	MUST be provided for XCA 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.

Table 3: epSOS Patient Summary Metadata

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 [epSOS D3.2.2]. 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). Due to this implied relationship between the provided documents, an explicit encoding of the document relationships MAY be omitted. 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-XCA. "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>
```

If a warning is to be transmitted to the HCP (see section 3.1.4) the ebXML Registry Error mechanism MUST be used with a syntax as defined in section 3.43.5 of [IHE ITI TF 2b]. 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	ResponseStatus	epSOS Warning Message (codeContext attribute)	Code (error-Code attribute)
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 HCP 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

3.3.1.5 Response Message (No Patient Summary Provided)

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]. 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. (ERROR)	Failure	No Consent	4701	The HCP 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, HCP SHOULD re-issue the request for medical data.
Country A requests a higher authentication trust level than assigned to the HCP (e.g. password-based login is not accepted for the requested operation). (ERROR)	Failure	Weak Authentication	4702	If possible, the HCP SHOULD log in again with a stronger mechansims (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 HCP (ERROR).	Failure	Insufficient Rights	4703	If the HCP can switch to another (approriate) role, he SHOULD do so and re-issue the request.
No patient summary is registered for the given patient. (WARNING)	Success	No Data	1102	-
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.

3.3.1.6 Example Response Message

The following message is a possible response to the sample request message given in section 3.3.1.2. 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>

            <!-- set to same value as Patient ID (required by XCA) -->
            <rim:Slot name="sourcePatientId">
                <rim:ValueList>

<rim:Value>90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;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>
            <!-- 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>
                <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 -  (34133-9) -->
            <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="34133-9">
                <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 -  (34133-9) -->
            <rim:Classification
                id="urn:uuid:87a7cfc2-a956-4d6e-af30-c7e78809c95f"
                lid="urn:uuid:87a7cfc2-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="34133-9">
                <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: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-a8ffeff98427"
                value="90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO"
                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>
                UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi.....
            </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">

            <!-- 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^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;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">
                <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-aca8dea078ef"
                lid="urn:uuid:89a73ab3-344a-4098-b827-aca8dea078ef"
                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"
                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 -->

            <!-- Class Code - Patient Summary (34133-9) -->
            <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="34133-9">
                <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 - Patient Summary (34133-9) -->
            <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="34133-9">
                <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"
                        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^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;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 -->
            <rimext:Document>
                UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi....
            </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>
```

3.3.2 Security Audit Considerations

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in section 4.5.3. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in section 4.5.4.

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	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

3.3.3 Protocol Requirements

The *epSOS Patient Service* List() request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in section 4.3 of this document.

Port types and bindings MUST be used as defined in the WSDL given in section 6.4.2 of this document. 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 section 6.4.2)
List response	CrossGatewayQueryRetrieveResponse_Message (see section 6.4.2)

The request message MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document. The response message MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document.

3.4 epSOS Order Service

The following change history provides an overview of all changes to chapter 3.4 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The epSOS Order Service is 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.

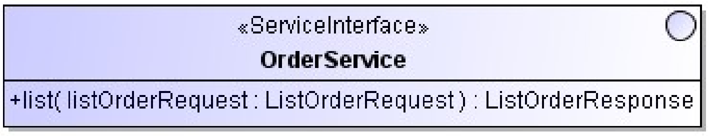

«ServiceInterface»
OrderService
+list(listOrderRequest : ListOrderRequest) : ListOrderResponse

Figure 11 - Order Service Interface

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[17] [OASIS ebRS 3.0]
- MTOM: SOAP Message Transmission Optimization Mechanism [W3C MTOM]
- XOP: XML-binary Optimized Packaging [W3C XOP]

and is an extension to the IHE profiles:

- XCA: IHE Cross-Community Access [IHE XCA]

For discovery and localisation of the Order Service instance that is responsible for providing access to the identified patient's data see section 2.1.4 of this document.

3.4.1 List() Operation

The *epSOS Order Service* list() operation is implemented as an extension to the IHE XCA Cross-Gateway Query 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).

3.4.1.1 Request Message

The list() request is initiated by an HCP in the country of care for retrieving the available ePrescription documents of an identified patient. The respective request message builds upon the IHE XCA Cross-Gateway Query request message.

[17] The integration of ebRS and MTOM as used by epSOS is not compatible with the current version of OASIS ebRS.

The <AdhocQueryRequest/> element that encapsulates the query parameters MUST be used as follows for epSOS:

Element Name	epSOS Usage Convention
ResponseOption/@returnComposedObjects	MUST be “true” (per XCA)
ResponseOption/@returnType	MUST be “leafClassWithRepositoryItem” (per epSOS extension, see section 3.1.2)
AdhocQuery	Container for holding the ebML stored query arguments. All arguments MUST be encoded as query slots (see table below).
AdhocQuery@id	MUST use the Find Documents query ID from Cross-Gateway Query transaction (XCA-ITI-38): "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d"

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.

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:ResponseStatusType:Approved'
$XDSDocumentEntryClassCode	R	ePrescription LOINC code ("57829-4") 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: '57829-4^^2.16.840.1.113883.6.1'
$XDSDocumentEntryTypeCode	O	ePrescription LOINC code ("57829-4") 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: '57829-4^^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 retuend by the service provider. If this stored query slot is omitted, the service provider MUST respond with all available encodings.
$IncludeAssociations	R/O	MUST be provided with a value of ‘yes’ if multiple encodings are requested. SHOULD be omitted if only a single encoding is requested.

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 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	urn:ihe:iti:xds-sd:pdf:2008	CDA-enveloped PDF/A encoding of the origin-

document		al document without any semantic transformation. The patient's country of affiliation MUST be able to provide the patient's available ePrescriptions in this format.

3.4.1.2 Example Request Message

The following excerpt from a epSOS Order Service list() request message shows an IHE XCA based Cross-Gateway query request that contains argument slots for retrieving the available ePrescriptions (LOINC code 57829-4) of an identified patient (patient identifier 90378912821). In this example the service consumer does not specify the requested encoding. Therefore the service provider MUST deliver both encodings (epSOS pivot and PDF/A) for all available ePrescriptions.

```
<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="$XDSDocumentEntryPatientId">
         <rim:ValueList>
            <rim:Value>
                '90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO'
            </rim:Value>
         </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="$XDSDocumentEntryStatus">
         <rim:ValueList>
            <rim:Value>
                ('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')
             </rim:Value>
         </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="$XDSDocumentEntryClassCode">
         <rim:ValueList>
            <rim:Value>('57829-4^^2.16.840.1.113883.6.1')
            </rim:Value>
         </rim:ValueList>
      </rim:Slot>
      <!-- Include associations whose sourceObject and targeObject attributes
         reference ExtrinsicObjects returned -->
      <rim:Slot name="$IncludeAssociations">
         <rim:ValueList>
            <rim:Value>'yes'</rim:Value>
         </rim:ValueList>
      </rim:Slot>
    </rim:AdhocQuery>
  </query:AdhocQueryRequest>
</soapenv:Body>
</soapenv:Envelope>
```

3.4.1.3 Expected Actions

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, see section 3.4.1.4) or
- an error message (no ePrescriptions provided, see section 3.4.1.5).

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 section 4.6 of this document.

3.4.1.4 Response Message (Full Success Scenario)

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 Query response and Cross-Gateway Retrieve Response messages, by creating a new combined QueryRetrieve message[18].. 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 XCA Cross-Gateway Stored Query response message [IHE XCA]
`@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” (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]
`../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 Table 4 below.
`../../../rimext:Document`	This is an epSOS specific extension to [IHE XCA]. 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] MUST be used. If no restrictions on metadata values are given, the metadata elements MUST be used as per [IHE XCA].

[18] A respective change request to include this extension with the IHE XCA profile has been agreed with the profile authors and proposed to IHE ITI Technical Committee.

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	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 “yyyymmdd”
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.
repositoryUniqueId	rim:Slot	O	SHOULD be omitted by the service provider and MUST NOT be processed by the service consumer.
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.
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 ("57829-4"). 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 XCA compatibility but MAY be ignored by the service consumer. Value SHOULD be set to “Not Used”.
formatCode	Classification	R	MUST be “urn:epSOS:ep:pre: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 XCA compatibility but MAY be ignored by the service consumer. Value SHOULD be set to “Not Used”..
practiceSettingCode	Classification	R	MUST be provided for XCA 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.

Table 4: epSOS ePrescription Metadata

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-XCA. “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"
  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>
```

If a warning is to be transmitted to the HCP (see section 3.1.4) the ebXML Registry Error mechanism MUST be used with a syntax as defined in section 3.43.5 of [IHE ITI TF 2b]. 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 HCP MAY request the source coded	PartialSuccess	Collection incomplete	4102	None

PDF. (ERROR)				
The HCP 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	IDs of the affected documents
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

3.4.1.5 Response Message (No ePrecriptions Provided)

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]. 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 HCP 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, HCP SHOULD re-issue the request for medical data.
Country A requests a higher authentication trust level than assigned to the HCP (e.g. password-based login is not accepted for the requested operation).	Failure	Weak Authentication	4702	If possible, the HCP SHOULD log in again with a stronger mechansims (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 HCP.	Failure	Insufficient Rights	4703	If the HCP can switch to another (approriate) 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 given argument values (ERROR)	Failure	Unknown Filter	4202	The service consumer MAY re-issue the request using another filter expression.

3.4.1.6 Example Response Message

In this section three possible response messages to the previously sketched request message 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 section 3.3.1.6 for 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"
            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-d07d16ddaeb9"
                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 firist 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[19].

```
<soapenc:Envelope>
   <soapenv:Header>....</soapenv:Header>
   <soapenv:Body>
     <query:AdhocQueryResponse
          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="urn:uuid:a1c7a9ac-83aa-4eaf-b5e3-d355b57a5016">
       </rs:RegistryErrorList>

       <rim:RegistryObjectList>

         <!-- ePrecription 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>

         <!-- ePrecription 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) -->
```

[19] It's 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.

```
         </rimext:ExtrinsicObject>

         <!-- ePrecription 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
                >UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</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"
            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-d07d16ddaeb9"
                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>
```

3.4.2 Security Audit Considerations

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in section 4.5.3. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in section 4.5.4.

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	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

3.4.3 Protocol Requirements

The *epSOS Order Service* List() request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in section 4.3 of this document.

Port types and bindings MUST be used as defined in the WSDL given in section 6.4.2 of this document. Acc. to this the *epSOS Order Service* List() operation’s request and response data MUST be contained within the message body as follows:

epSOS Order Service	Message Body
List request	CrossGatewayQueryRetrieve_Message (see section 6.4.2)
List response	CrossGatewayQueryRetrieveResponse_Message (see section 6.4.2)

The request message MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document. The response message MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document.

3.5 epSOS Dispensation Service

The following change history provides an overview of all changes to chapter 3.5 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The *epSOS Dispensation Service* is 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.

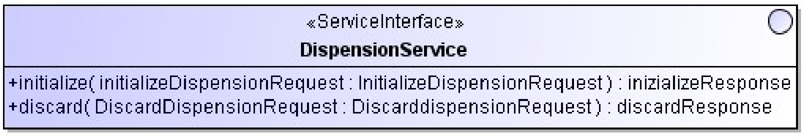

«ServiceInterface»
DispensionService
+initialize(initializeDispensionRequest : InitializeDispensionRequest) : inizializeResponse
+discard(DiscardDispensionRequest : DiscarddispensionRequest) : discardResponse

Figure 12 - DispensationInterface

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 [OASIS ebRS 3.0]
- 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 section 2.1.4 of this document.

3.5.1 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].

3.5.1.1 Request Message

The initialize() request is initiated by an HCP 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
`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 (pointers to) all eDispensation documents
`../../ExtrinsicObject`	For each eDispensation document a single extrinsic object MUST be defined. There MUST be a 1:1 id-correspondence between <rim:ExtrinsicObject> elements and <ihe:Document> elements. For a list of further metadata to be provided with an eDispensation document see the table below.
`../../../Document`	base64encoded data for the eDispensation documents being submitted to the service provider. The <rimext:Document/> 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.
`../../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]. 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	Identifer of the document. This identifier MUST be the same for <rim:ExtrinsicObject/@id> and <ihe:Document/@id>.
mimeType	Attribute	MUST be "text/xml"
objectType	Attribute	MUST be set acc. to section 4.3.1.2 of [IHE IT TF 3]
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 XDR compatibility but MAY be ignored by the service consumer. Value SHOULD be set to "Not Used".
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. Value SHOULD be set to "Not Used".
XDSDocumentClassCode	classification	eDispensation LOINC code ("DISPN-X")[20] 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 <ihe:Document> element.

Other metadata than the ones listed above SHOULD NOT be provided by the service provider[21]. 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-XCA. 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"
```

[20] This code is a dummy that will be used for the intial NCP integration tests until a eDispensation LOINC code is approved.

[21] 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.

```
   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>
```

3.5.1.2 Example Request Message

The following excerpt from a *epSOS Dispensation Service* InitializeRequest message shows the transmission of a single eDispensation document (with two encodings) before MTOM optimization tales place:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns=...>
<soapenv:Header> ... </soapenv:Header>
<soapenv:Body>
  <xds:ProvideAndRegisterDocumentSetRequest xmlns=...>
    <lcm:SubmitObjectsRequest>
        <rim:RegistryObjectList>


            <!-- Linkage between objects shown with symbolic names instead of
                 UUIDs to make the linkage easier to read and understand.
                 The Document Recipient will insert UUIDs for the symbolic names
                 upon receipt -->

            <!-- epSOS pivot CDA eDispensation document -->
            <rimext:ExtrinsicObject id="epSOS Document"
                objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
                mimeType="text/xml">

                <!-- These attributes are required by XDR but not used by epSOS.
                     They are shown in this example so it is a valid XDR
                     message.  They will be ignored by the epSOS Document
                     Recipient -->

                <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 XDR -->
                <rim:Slot name="sourcePatientId">
                    <rim:ValueList>
                        <rim:Value>
                        90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO
                        </rim:Value>
                    </rim:ValueList>
                </rim:Slot>

                <!-- HealthcareFacilityType Code  -->
                <rim:Classification id="xpscl8"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"
                    classifiedObject="epSOS Document"
                    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>

                <!-- PracticeSetting Code  -->
                <rim:Classification id="xpscl9"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead"
                    classifiedObject="epSOS Document"
                    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="xpscl10"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
                    classifiedObject="epSOS Document"
                    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 -->

                <!-- Class Code - eDispensation (DISPN-X) -->
                <rim:Classification id="xcc22"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
                    classifiedObject="epSOS Document"
                    nodeRepresentation="DISPN-X">
                    <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="eDispensation"/>
                    </rim:Name>
                </rim:Classification>

                <!-- Type Code - eDispensation (DISPN-X) -->
                <rim:Classification id="xcc23"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983"
                    classifiedObject="epSOS Document"
                    nodeRepresentation="DISPN-X">
                    <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="eDispensation"/>
                    </rim:Name>
                </rim:Classification>

                <!-- Format Code -->
                <rim:Classification
                    id="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="epSOS Document"
                    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 xml:lang="en" charset="UTF-8"
                            value="epSOS coded eDispensation"/>
                    </rim:Name>
                </rim:Classification>

                <!-- Patient ID -->
                <rim:ExternalIdentifier
                    id="urn:uuid:982f1551-5901-4bc5-8870-801181941817"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
                    identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
                   value="90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO"
                    registryObject="epSOS Document">
                    <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"
                    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 Document">
                    <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>
                   UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi....
                </rimext:Document>
            </rimext:ExtrinsicObject>


            <!-- epSOS source coded CDA wrapped PDF eDispensation document -->
            <rimext:ExtrinsicObject id="OriginalDocument"
                objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
                mimeType="text/xml">

                <!-- These attributes are required by XDR but not used by epSOS.
                     They are shown in this example so it is a valid XDR
                     message.  They will be ignored by the epSOS Document
                     Recipient -->

                <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 XDR) -->
                <rim:Slot name="sourcePatientId">
                    <rim:ValueList>
                        <rim:Value>
                          90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO
                        </rim:Value>
                    </rim:ValueList>
                </rim:Slot>

                <!-- HealthcareFacilityType Code  -->
                <rim:Classification id="pscl8"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"
                    classifiedObject="OriginalDocument"
                    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>

                <!-- PracticeSetting Code  -->
                <rim:Classification id="pscl9"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead"
                    classifiedObject="OriginalDocument"
                    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="pscl10"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
                    classifiedObject="OriginalDocument"
                    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 -->

                <!-- Class Code - eDispensation (DISP-X) -->
                <rim:Classification id="pscl1"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
                    classifiedObject="OriginalDocument"
                    nodeRepresentation="DISP-X">
                    <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="eDispensation"/>
                    </rim:Name>
                </rim:Classification>

                <!-- Type Code - eDispensation (DISP-X) -->
                <rim:Classification id="pscl3"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983"
                    classifiedObject="OriginalDocument"
                    nodeRepresentation="DISP-X">
                    <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="eDispensation"/>
                    </rim:Name>
                </rim:Classification>

                <!-- Format Code -->
                <rim:Classification id="pscl2"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d"
                    classifiedObject="OriginalDocument"
                    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"
                            value="PDF/A coded document"/>
                    </rim:Name>
                </rim:Classification>

                <!-- Patient ID -->
                <rim:ExternalIdentifier id="psei1"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
                    identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
                   value="90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO"
                    registryObject="OriginalDocument">
                    <rim:Name>
                        <rim:LocalizedString xml:lang="en-us" charset="UTF-8"
                            value="XDSDocumentEntry.patientId"/>
                    </rim:Name>
                </rim:ExternalIdentifier>

                <!-- Unique ID -->
                <rim:ExternalIdentifier id="psei2"
                    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="OriginalDocument">
                    <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>
                   UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi....
                </rimext:Document>
            </rimext:ExtrinsicObject>

            <!-- The Summary document is a Transformation of the OriginalDocument.
             -->
            <rim:Association id="xfrm_assoc"
                associationType="urn:ihe:iti:2007:AssociationType:XFRM"
                sourceObject="epSOS Document"
                targetObject="OriginalDocument">
                <rim:Classification id="urn:uuid:8ec64c7e-8b7d-4d63-8741-c5a5890e5af3"
                    classificationScheme="urn:uuid:abd807a3-4432-4053-87b4-fd82c643d1f3"
                    classifiedObject="xfrm_assoc"
                    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>

            <!-- The SubmissionSet is necessary as a 'wrapper' around metadata
                 submissions -->
            <rim:RegistryPackage id="SubmissionSet01"
                objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:RegistryPackage">

                <rim:Slot name="submissionTime">
                    <rim:ValueList>
                        <rim:Value>20100525</rim:Value>
                    </rim:ValueList>
                </rim:Slot>

                <!-- Content Type Code -->
                <rim:Classification
                    classificationScheme="urn:uuid:aa543740-bdda-424e-8c96-df4873be8500"
                    classifiedObject="SubmissionSet01"
                    nodeRepresentation="epSOS ePrescription"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
                    id="id_12">
                    <rim:Slot name="codingScheme">
                        <rim:ValueList>
                            <rim:Value>epSOS contentTypeCodes</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Name>
                        <rim:LocalizedString value="ePrescription"/>
                    </rim:Name>
                </rim:Classification>

                <!-- Unique ID -->
                <rim:ExternalIdentifier
                    identificationScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8"
                    value="1.2009.0827.08.33.5017"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
                    id="id_13"
                    registryObject="SubmissionSet01">
                    <rim:Name>
                        <rim:LocalizedString value="XDSSubmissionSet.uniqueId"/>
                    </rim:Name>
                </rim:ExternalIdentifier>

                <!-- Source ID -->
                <rim:ExternalIdentifier
                    identificationScheme="urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832"
                    value="1.3.6.1.4.1.21367.2009.1.2.1"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
                    id="id_14" registryObject="SubmissionSet01">
                    <rim:Name>
                        <rim:LocalizedString value="XDSSubmissionSet.sourceId"/>
                    </rim:Name>
                </rim:ExternalIdentifier>

                <!-- Patient ID -->
                <rim:ExternalIdentifier
                    identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446"
                    value="90378912821^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO"
                    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
                    id="id_15" registryObject="SubmissionSet01">
                    <rim:Name>
                        <rim:LocalizedString value="XDSSubmissionSet.patientId"/>
                    </rim:Name>
                </rim:ExternalIdentifier>
            </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 two DocumentEntries (ExtrinsicObjects) included must be part of the
                 SubmissionSet. The following associations make this so -->
            <rim:Association
                associationType="urn:oasis:names:tc:ebxml-
regrep:AssociationType:HasMember"
                sourceObject="SubmissionSet01"
                targetObject="epSOS Document"
                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:Association
                associationType="urn:oasis:names:tc:ebxml-
regrep:AssociationType:HasMember"
                sourceObject="SubmissionSet01"
                targetObject="OriginalDocument"
                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>
```

3.5.1.3 Expected Actions

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 section 4.6 of this document.

3.5.1.4 Response Message (Full Success Scenario)

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"

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

3.5.1.5 Response Message (Failure or Partial Failure Scenario)

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 eDispensations was processed succesfully, 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.

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] 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	HCP-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	HCP-B SHOULD again query for the list of available ePrescription.
Country A requests a higher authentication trust level than assigned to the HCP (e.g. password-based login is not accepted for the requested operation). (ERROR)	-	Weak Authentication	4702	If possible, the HCP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
The eDispensation service provider only accepts dispensation data that	OID of the eDispensation docu-	No Signature	4704	If possible, NCP-B SHOULD re-issue the request with the

is digitally signed by an HCP. (ERROR)	ment that caused the error.			data signed by an HCP.
The service consumer did not provide the source coded PDF document for an eDispensation (ERROR)	OID of the epSOS coded eDispensation that in not additionaly provided as source coded document	Original data missing	4107	The epSOS pivot coded document MUST NOT be processed by the service provider. The service consumer 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 in not additionaly provided as epSOS pivot coded document	Pivot data missing	4108	The source coded document MUST NOT be processed by the service provider. The servie consumer MUST re-transmit the dispensation with both encodings.

3.5.1.6 Example Response Message

The following example shows a possible positive resonse to the request given in section 3.5.1.2:

```
<?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 resonse to the request given in section 3.5.1.2:

```
<?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="1.42.20100103225206.3.3" />
     </rs:RegistryErrorList>
   </rs:RegistryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

3.5.1.7 Security Audit Considerations

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in section 4.5.3. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in section 4.5.4.

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:

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

3.5.2 Discard() Operation

The *epSOS Dispensation Service* discard() operation can be used to deprecate a previously transmitted eDispensation. It is implemented by the ebXML RemoveObjectsRequest registry operation as profiles in the IHE Draft Profile on XDS Metadata Update [IHE XDS Update].

3.5.2.1 Request Message

The *epSOS Dispensation Service* discard() request is initiated by an HCP 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 Update]:

Element Name	epSOS Usage Convention
`ObjectRefList`	List of all eDispensation objects that have been errornously sent to country A
`../ObjectRef`	For each eDispensation object, submission set and association to discard there MUST be a single ObjectRef element
`../ObjectRef/@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

3.5.2.2 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 section 3.5.1.2).

```
<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  -->
          <ObjectRef id="urn:uuid:822441f0-1644-42bf-9dce-f718598beb13"/>

          <!-- SubmissionSet -->
          <ObjectRef id="urn:uuid:cafddedb-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>
```

3.5.2.3 Expected Actions

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 HCPO 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 section 4.6 of this document.

3.5.2.4 Response Message (Full Success Scenario)

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>
```

3.5.2.5 Response Message (Failure or Partial Failure Scenario)

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 succesfully, 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.

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] 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 HCP 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. HCP and patient MUST be aware that the respective prescription cannot be dispensed again immediately.

3.5.2.6 Example Response Message

The following example shows a possible positive response to the request given in section 3.4.1.2:

```
<?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 section 3.4.1.2:

```
<?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="1.42.20100103225206.3.3" />
     </rs:RegistryErrorList>
   </rs:RegistryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

3.5.2.7 Security Audit Considerations

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in section 4.5.3. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in section 4.5.4.

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

3.5.3 Protocol Requirements

The *epSOS Dispensation Service* request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in section 4.3 of this document.

Port types and bindings MUST be used as defined in the WSDLs given in sections 6.4.3 (put operation) and 6.4.4 (discard operation) of this document. Acc. to this the *epSOS Dispensation 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 section 6.4.3)
Put response	ProvideAndRegisterDocumentSet-bResponse_Message (see section 6.4.3)
Discard request	DeleteMetadata_Message (see section 6.4.4)
Discard response	DeleteMetadataResponse_Message (see section 6.4.4)

epSOS Dispensation Service request messages MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document. *epSOS DispensationService* response messages MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document.

3.6 epSOS Consent Service

The following change history provides an overview of all changes to chapter 3.6 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The *epSOS Consent Service* is 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.

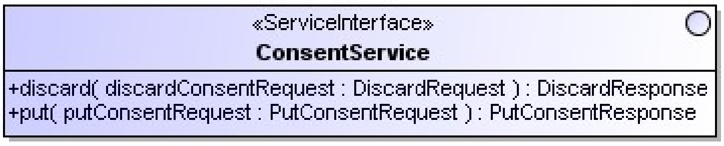

«ServiceInterface»
ConsentService
+discard(discardConsentRequest : DiscardRequest) : DiscardResponse
+put(putConsentRequest : PutConsentRequest) : PutConsentResponse

Figure 13 - Consent Service Interface

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]

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]

For discovery and localisation of the *epSOS Consent Service* instance that is responsible for providing access to the identified patient's data see section 2.1.4 of this document.

3.6.1 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].

3.6.1.1 Request Message

The put() request is initiated by an HCP 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 consists of a *Patient Privacy Consent Acknowledgment Document* acc. to section 5.1 of [IHE ITI TF-3] and an optional *Scanned Document Part* acc. to section 5.2 of [IHE ITI TF-3].

The *epSOS Consent Service* PutRequest 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 <ExtrinsicObject> element that holds the metadata for the transmitted consent document.
../../ExtrinsicObject	A single Patient Privacy Consent Acknowledgment Document MAY be transmitted. The <ExtrinsicObject> element holds all metadata for this document. Metadata and classifications MUST comply with sections 5.1 and 5.2 of [IHE ITI TF3]. 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 <rimext:Document/> 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.

The service consumer MAY wrap the provided document as a single IHE XDS submission set [IHE ITI TF-2a] 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]:

Metadata element	Binding	Slot Value
id	Attribute	Identifer of the document. This identifier MUST be the same for <rim:ExtrinsicObject/@id> and <ihe:Document/@id>.
mimeType	Attribute	MUST be "text/xml"

objectType	Attribute	MUST be set acc. to section 4.3.1.2 of [IHE ITI TF-3]
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 XDR compatibility but MAY be ignored by the service consumer. Value SHOULD be set to "Not Used".
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. Value SHOULD be set to "Not Used".
$XDSDocumentClassCode	classification	MUST be "Consent“
$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 Identification Service* (encoded as HL7 v3 II data type)
$XDSDocument.EntryUUID	External identifier	MUST refer to the UUID of the corresponding <ihe:Document> element.
$XDSDocument.UniqueId	External identifier	MUST refer to the OID of the CDA document that is included within the <ihe:Document> 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.

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 HCPs 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 HCPs of the current country of care to access his medical data by the means of epSOS.

3.6.1.2 Example Request Message

The following excerpt from a *epSOS Consent Service* PutRequest message shows the transmission of a Patient Privacy Consent Acknowledgment Document (without scanned document part). As most of the metadata is similar to the already shown transmission of an eDispensation, 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"
             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="Consent"/>
                </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="Consent"/>
                </rim:Name>
                <rim:Description/>
                <rim:VersionInfo versionName="1.1"/>
             </rim:Classification>

             <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>
                UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi....
             </rimext:Document>
           </rim:ExtrinsicObject>

           <!-- The SubmissionSet is necessary as a 'wrapper' around metadata
                submissions -->
           <rim:RegistryPackage id="SubmissionSet01"
               objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:RegistryPackage">

           <!-- submission set metadate 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>
```

3.6.1.3 Expected Actions

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 section 4.6 of this document.

3.6.1.4 Response Message (Full Success Scenario)

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 responds with an *ebXML Registry Response* with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

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

3.6.1.5 Response Message (Failure or Partial Failure Scenario)

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 ”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]. 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 HCP (e.g. password-based login is not accepted for the requested operation).	Weak Authentication	4702	If possible, the HCP SHOULD log in again with a stronger mechansims (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 HCP 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 HCP SHOULD re-issue the request after the general consent has been set operational.

3.6.1.6 Example Response Message

The following example shows a possible positive response to the request given in section 3.5.1.2:

```
<?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 section 3.5.1.2:

```
<?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>
```

3.6.1.7 Security Audit Considerations

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in section 4.5.3. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in section 4.5.4.

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	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 "4" (Resource)
ParticipantObjectIDTypeCode	R	MUST be "12" (URI)
ParticipantObjectID	R	MUST be string-encoded UUIDs of the provided document

3.6.2 Discard() Operation

The *epSOS Consent Service* discard() operation can 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 [IHE XDS Update].

3.6.2.1 Request Message

The *epSOS Consent Service* discard() request is initiated by an HCP 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 Update]:

Element Name	epSOS Usage Convention
`ObjectRefList`	Wrapper on the consent that has been errornously 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

../ObjectRef/@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 have to be referenced in the <ObjectRefList>:

- Consent document (with or without scanned consent)
- Submission set
- Associations between consent document and the submission set

3.6.2.2 Example Request Message

For an example on the use of the ebXML RemoveObjectsRequest message for discarding erroneously transmitted epSOS documents see section 3.5.2.2.

3.6.2.3 Expected Actions

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 HCP 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 section 4.6 of this document.

3.6.2.4 Response Message (Full Success Scenario)

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>
```

3.6.2.5 Response Message (Failure or Partial Failure Scenario)

If the *epSOS Consent Service* provider is able to decode the received consent document IDs but the deprecating of the consent document 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 ”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]. 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 HCP 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	HCPO SHOULD ensure that the discard request is issued by the same person who accepted the original consent. If consent was given at another HCPO the patient MUST request for discarding at this HCPO.
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 od a consent the HCP SHOULD ask the patient for a reverse consent (e.g. Opt-Out in case of an errorneously sent Opt-In consent) and send this consent to country A by using the put() operation.

3.6.2.6 Example Response Message

For an example on the use of the ebXML RemoveObjectsRequest message for discarding erroneously transmitted epSOS documents see section 3.5.2.2.

3.6.2.7 Security Audit Considerations

The service consumer MUST write an audit trail entry according to the HCP Assurance Audit Schema as defined in section 4.5.3. The service provider MUST write an audit trail entry according to the Patient Privacy Audit Schema as defined in section 4.5.4.

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 consent document

3.6.3 Protocol Requirements

The *epSOS Consent Service* request and response messages will be transmitted using synchronous Web Services Exchange, according to the requirements specified in section 4.3 of this document.

Port types and bindings MUST be used as defined in the WSDLs given in sections 6.4.3 (initialize operation) and 6.4.4 (discard operation) of this document. Acc. to this the *epSOS Consent Service* operations' request and response data MUST be contained within the message body as follows:

epSOS Consent Service	**Message Body**
Initialize request	ProvideAndRegisterDocumentSet-b_Message (see section 6.4.3)
Initialize response	ProvideAndRegisterDocumentSet-bResponse_Message (see section 6.4.3)
Discard request	DeleteMetadata_Message (see section 6.4.4)
Discard response	DeleteMetadataResponse_Message (see section 6.4.4)

epSOS Consent Service request messages MUST be protected by the service consumer (NCP-B) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document. *epSOS Consent Service* response messages MUST be protected by the service provider (NCP-A) according to the epSOS message security considerations as defined in section 4.3.5.2 of this document.

4 epSOS Communication and Messaging 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 (Figure 14).

Figure 14: epSOS Trusted Nodes and Messaging Infrastructure

The epSOS trusted node infrastructure implements the core epSOS security services that 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
- mutual NCP authentication

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 HCP attributes
- common message format
- signature on message elements for auditing and brokering of document authenticity claims

It must be noted that only NCPs acting as epSOS service providers and consumers are part of the epSOS trusted node infrastructure as specified in this document. 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.

4.1 Trusted Node Infrastructure

The following change history provides an overview of all changes to chapter 4.1 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

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[22] [RFC 2246]
- IHE Audit Trail and Node Authentication [IHE ITI TF-2a]

[22] 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.

4.1.1 IPSec Configuration

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 section 5.1 of this document. Gateway certificates MUST comply with the certificate profiles as defined in sections 5.4.3 and 5.4.4 of this document. The issuing 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]).

4.1.2 TLS configuration

All network nodes running epSOS service consumers or service providers MUST be implemenented 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]).

With respect to the ITI-19 transaction specification the following constraints and extensions apply:

- Algorithms and key lengths MUST be used acc. to section 5.1 of this document.
- The node certificates MUST comply with the epSOS Node Authentication Certificate Profile (see sections 5.4.5 and 5.4.6 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]).

4.2 Time Synchronisation

The following change history provides an overview of all changes to chapter 4.2 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

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]

Stratum 2 time servers (*Consistent Time Mediators)* SHOULD by 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

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.

4.3 epSOS Common Message Format

The following change history provides an overview of all changes to chapter 4.3 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

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.

4.3.1 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 section 4.1).

4.3.2 Message Layer Profile

The epSOS Common Message Format is a SOAP 1.2 [W3C SOAP 1.2] message contained as the body of an HTPP 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[23].

All epSOS SOAP messages MUST comply with the WS-I Basic Profile 1.1[24] [WSI BP 1.1].

All epSOS SOAP messages MUST comply with the WS-I Basic Security Profile 1.1 [WSI SBP 1.1].

4.3.3 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).

4.3.4 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".

[23] 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.

[24] 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.

All SOAP Bindings in the WSDL MUST specify use="literal".

The naming of the messages MUST be as defined for the used standard.

4.3.5 Embedding of Security Token

Each SOAP message MUST include a <wsse:Security> section within the SOAP header.

4.3.5.1 SAML Assertions

Request messages are safeguarded by up to two SAML assertions that attest the authenticity of the user and the existence of a treatment relationship (See chapter 2 on which assertions are required for each operation).

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 section 5.3.1). 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.

4.3.5.2 Message Signature

To preserve the integrity and authenticity of a message and to attest the NCP origin of the message, elements of each message MUST 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[25].

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 section 3.1.6 of this document MUST NOT be used.
SignatureMethod	The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see section 5.1). 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.
DigestMethod	The hash algorithm MUST comply with the epSOS recommendations on algorithms and key lengths (see section 5.1). For signing message elements the digest method • "http://www.w3.org/2000/09/xmldsig#sha1" • http://www.w3.org/2001/04/xmlenc#sha256

[25] Only in cases where the framework does not allow for multiple XPath expressions, a signed parts assertion SHOULD be used.

	SHOULD be used. A country MAY reject SHA-1 digests.
KeyInfo	This element MUST contain a wsse:SecurityTokenReference element which references the protection token.

4.3.6 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.

4.4 epSOS Trusted Service List

The following change history provides an overview of all changes to chapter 4.4 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

Network addresses, web service endpoints and certificates of a country's epSOS service providers and consumers are registered within a NCP Service Status List (NSL) that is digitally signed by a trusted authority of the respective country (see [epSOS D3.7.2] for details). epSOS NSLs of all member states are part of each NCPs configuration. How an NCP obtains these NSLs is out of the scope of this specification and will be described as part of the epSOS operational and administrative guidelines.

epSOS NSLs are encoded as ETSI Trust-service Status Lists acc to [ETSI TS 102 231]. Figure 15 shows how the ETSI TSL structure is used to provide information on epSOS services.

Figure 15: ETSI TSL for encoding epSOS service status information

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 sections define the application of [ETSI TS 102 231] for encoding epSOS NCP-Service Status Lists. For a complete example of an epSOS NCP Service Status List see Appendix 6.3.3 of this document.

4.4.1 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 Appendix .....)
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: *Countryname* (*Countrycode)*” (for the use of country codes see Appendix .....). The scheme name MUST be provided in 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 Appendix .....)
	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 (see section ...)
	TrustServiceProvider	O	Information on NCP-B gateways and services (see section ...)
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 section 3.1.6 of this document MUST NOT be used.
SignatureMethod	The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see section ...). 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 section ....). 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.

4.4.2 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	M	M	
epSOS NCP	M	M	
epSOS Patient Identification Service	M	-	
epSOS Patient Service	O	-	
epSOS Order Service	O	-	
epSOS Dispensation Service	O	-	
epSOS Consent Service	O	-	
HCP Identity Provider	-	O	
HCP Signature CA	O	O	

4.4.3 epSOS VPN Gateway Status Information

epSOS VPN Gateways status information entries are used to announce the address and digital ceritficate 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 section ... of this document.
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”.
StatusStartingTime	R	MUST be used acc. to [ETSI TS 102 231].
SchemeServiceDefinitionURI	-	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	-	MUST NOT be used for epSOS.
ServiceInformationExtension	-	MUST NOT be used for epSOS.
ServiceHistory	-	MUST NOT be used for epSOS.

Other fields than the ones listed above MUST NOT be provided for epSOS VPN Gateway status information.

4.4.4 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 in section 5.4.6 of this document. For NCP-B each of these MUST comply with the epSOS TLS client certificate profile as defined in section 5.4.5 of this document.
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 section 5.4.7 of this document.
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	-	MUST NOT be used for epSOS.
ServiceSupplyPoints	-	MUST NOT be used for epSOS.

TSPServiceDefinitionURI	-	MUST NOT be used for epSOS.
ServiceInformationExtension	-	MUST NOT be used for epSOS.
ServiceHistory	-	MUST NOT be used for epSOS.

Other fields than the ones listed above MUST NOT be provided for epSOS NCP status information.

4.4.5 epSOS Service Status Information

Service status information is used for announcing the web service enedpoint addresses of the epSOS services.

TSL Element	Opt	Usage Convention
TSPService	R	
ServiceInformation	R	
ServiceTypeIdentifier	R	MUST be used as follows: PatientIdentificationService service provider: “http://uri.epsos.eu/Svc/Svctype/PatientIdentificationService epSOS PatientService service provider: “http://uri.epsos.eu/Svc/Svctype/PatientService epSOS OrderService service provider: “http://uri.epsos.eu/Svc/Svctype/OrderService epSOS DispensationService service provider: “http://uri.epsos.eu/Svc/Svctype/DispensationService epSOS ConsentService service provider: “http://uri.epsos.eu/Svc/Svctype/ConsentService
ServiceName	R	MUST be used acc. to [ETSI TS 102 231].
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	-	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	-	MUST NOT be used for epSOS.
ServiceInformationExtension	-	MUST NOT be used for epSOS.
ServiceHistory	-	MUST NOT be used for epSOS.

Other fields than the ones listed above MUST NOT be provided for epSOS service status information.

4.4.6 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/IdV
		ServiceName		R	MUST be used acc. to [ETSI TS 102 231].
		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 section ... of this document.
		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		-	MUST NOT be used for epSOS.
		ServiceSupplyPoints		-	MUST NOT be used for epSOS.
		TSPServiceDefinitionURI		-	MUST NOT be used for epSOS.
		ServiceInformationExtension		-	MUST NOT be used for epSOS.
		ServiceHistory		-	MUST NOT be used for epSOS.

Other fields than the ones listed above MUST NOT be provided for epSOS IdP status information.

4.5 Audit Trail

The following change history provides an overview of all changes to chapter 4.5 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

All epSOS service consumers and service providers MUST write audit trail entries for all message exchange operations. 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 physician’s reputation and to save 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.

4.5.1 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 concete use of [RFC 3881] epSOS borrows coded values and extension mechansims 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]

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 compatibiluty could not be reached due to the extended requirements of epSOS on privacy and non-repudiation [epSOS D3.7.2].

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).`

4.5.2 RFC 3881 Overview and epSOS Audit Schemas

[RFC 3881] defines five categories that are subject to audit activity:

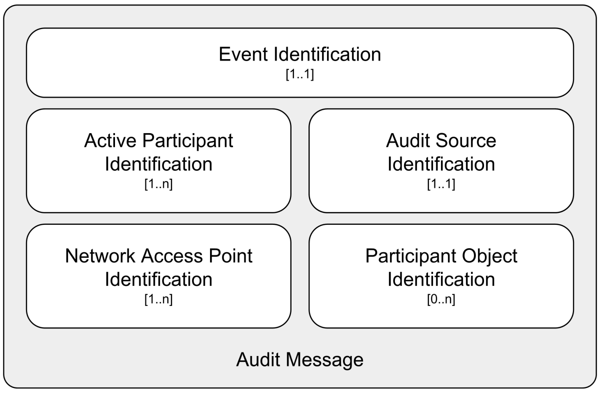

Event Identification
[1..1]
Active Participant Identification
[1..n]
Audit Source Identification
[1..1]
Network Access Point Identification
[1..n]
Participant Object Identification
[0..n]
Audit Message

Figure 16: RFC3881 overview

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?

For epSOS three different Audit Trail schemas are derived from these RFC 3881 categories. Table 5 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 HCPs in order to protect them against false accusations for not properly using the possibilities of epSOS (e. g. a patient claiming that a HCP 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).

Table 5: epSOS Audit Schemas

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 and service level agreements.

The following chapters will discuss each schema in respect to epSOS specific requirements and aspects.

4.5.3 epSOS HCP Assurance Audit Schema

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 Care	Point of Care that is the origin of the event
	Human Requestor	HCP 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 sections 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.

4.5.3.1 Event Identification

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(*num*, “epSOS Transaction”, *name*) where *num* is the number of the transaction including the “epSOS-“ prefix and *name* is the name of the transaction as written in the respective Use Case Roles diagram. See section 4.5.8.1 for a full list of all EventIDs defined for epSOS.
EventActionCode	R	Acc. RFC 3881. See section 4.5.8.1 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.

4.5.3.2 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 section 5.2).

UserIsRequestor	R	“true”
RoleIDCode	R	RFC 3881 compliant encoding of the kind of HCPO as defined in the “HCPO Type” attribute of the Authentication Assertion that was issued for the user.

4.5.3.3 Active Participant Identification: Human Requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HCP 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 section 4.5.8.3 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HCP as given in the Subject-ID attrbute of the HCP identity assertion (see section 5.2.3).
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.
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.

4.5.3.4 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”

4.5.3.5 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”

4.5.3.6 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.

4.5.3.7 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.

4.5.3.8 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.

4.5.3.9 Participant Object: Event Target

This subcategory MUST be defined individually for each transaction.

4.5.4 epSOS Patient Privacy Audit Schema

The Patient Privacy 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	HCP who triggered the event
	Service Comsumer 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 sections 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.

4.5.4.1 Event Identification

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(*num*, “epSOS Transaction”, *name*) where *num* is the number of the transaction including the “epSOS-“ prefix and *name* is the name of the transaction as written in the respective Use Case Roles diagram. See section 4.5.8.1 for a full list of all eventIDs defined for epSOS.
EventActionCode	R	Acc. RFC 3881. See section 4.5.8.1 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.

4.5.4.2 Active Participant Identification: Human Requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HCP 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 section 4.5.8.3 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HCP as given in the Subject-ID attrbute of the HCP identity assertion (see section 5.2.3).
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.

4.5.4.3 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”

4.5.4.4 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”

4.5.4.5 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.

4.5.4.6 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.

4.5.4.7 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.

4.5.4.8 Participant Object: Event Target

This subcategory MUST be defined individually for each transaction.

4.5.5 epSOS Patient ID Mapping Audit Schema

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	HCP 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 sections 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.

4.5.5.1 Event Identification

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(*num*, “epSOS Transaction”, *name*) where *num* is the number of the transaction including the “epSOS-“ prefix and *name* is the name of the transaction as written in the respective Use Case Roles diagram. See section 4.5.8.1 for a full list of all eventIDs defined for epSOS.
EventActionCode	R	Acc. RFC 3881. See section 4.5.8.1 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.

4.5.5.2 Active Participant Identification: Human Requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HCP 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 section 4.5.8.3 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HCP as given in the Subject-ID attrbute of the HCP identity assertion (see section 5.2.3).
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.

4.5.5.3 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”

4.5.5.4 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”

4.5.5.5 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”

4.5.5.6 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.

4.5.5.7 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.

4.5.5.8 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.

4.5.5.9 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.

4.5.6 Audit Trail Data for Non-Repudiation

For traceability and non-repudiation of message exchange operations, [epSOS 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 add the following sections to the message audit trail entries of all epSOS audit schemas as specified above.

4.5.6.1 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.

4.5.6.2 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.

4.5.7 Audit Trail Entries on Internal Activities

4.5.7.1 Issuance of a HCP Identity Assertion

The national Identity Provider service MUST write an audit trail entry for the confirmation of a HCP 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 section 4.5.3. 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 section 4.5.8.1 for the respective values.
Requesting Point of Care	R	Organisation that performed the initial identification and authentication of the HCP (e. g. a hospital)
Human Requestor	R	HCP whose authenticity was attested
Source Gateway	O	Service that performed the original authentication of the HCP
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 uses to identify active participants
Patient	X	
Event Target	R	See below

Table 6: Contry-B Identity Provider Audit Message Categories

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

4.5.7.2 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 HCP(O) and a patient. The audit message MUST be assembled according to the HCP Assurance audit schema as defined in section 4.5.3. 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 section 4.5.8.1 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	HCP who acts on behalf of the HCPO.
Source Gateway	O	System at the HCPO 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 uses to identify active participants
Patient	R	Patient who is treated by the HCPO
Event Target	R	See below

Table 7: Contry-B TRC Assertion Provider Audit Message Categories

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

4.5.7.3 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 section 4.5.3. 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 section 4.5.8.1 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	X	
Patient	X	
Event Target	R	See below

Table 8: epSOS NSL Import Audit Message Categories

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

4.5.7.4 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 section 4.5.3. 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 section 4.5.8.1 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	X	
Patient	X	
Event Target	R	See below

Table 9: epSOS Pivot Translation Audit Message Categories

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.

4.5.8 epSOS-specific Codes and Encodings

In the following sections epSOS-specific code lists and encoding conventions for use within audit trail entries are defined.

4.5.8.1 epSOS EventIDs

Service	Operation	Event ID	Êvent Name	Action
epSOSIdentificationService	FindIdentity-ByTraits	epsos-11	epsosIdentityService::FindIdentityByTraits	“E”
epSOSPatientService	List	epsos-21	epsosPatientService::List	“R”
epSOSOrderService	List	epsos-31	epsosOrderService::List	“R”
epSOSDispensationService	Initialize	epsos-41	epsosDispensationService::Initialize	“U”

	Discard	epsos-42	epsosDispensationService::Discard	“D”
epSOSConsentService	Put	epsos-51	epsosConsentService::Put	“U”
	Discard	epsos-52	epsosConsentService::Discard	“D”
Contry-B Identity Provider	Issuance of HCP Identity Assertion	epsos-91	identityProvider::HcpAuthentication	“E”
Country-B NCP	Issuance of a TRC Assertion	epsos-92	ncp::TrcAssertion	“E”
Configuration Manager	NSL Import	epsos-93	ncpConfigurationManager::ImportNSL	“E”
Transformation Manager	Pivot Translation	epsos-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.

4.5.8.2 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

4.5.8.3 Encoding of the User Identifier

The HCP 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.

4.6 Exception Handling

The following change history provides an overview of all changes to chapter 4.6 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

In general epSOS distinguishes between four coarse grained failure situations that MAY require an exchange of respective fault messages between NCPs:

- Communication failures: The message cannot be delivered to the designated service; e.g. because the establishment of a secure communication link failed or a link is broken.
- epSOS Message encoding and consistency failures: The message was received but it cannot be processed; e.g. because the security token is broken or the message does not comply with the epSOS message encoding and security rules

- Message processing failures: The message was decoded but it cannot be processed; e.g. because of security/privacy reasons or because the request does not match with the states of the affected security and business objects
- Document encoding failures: The message can be processed but the requested document cannot be completely encoded as specified in [epSOS D3.5.2C].

General system failures are handled basd on their implication (e.g. if a message cannot be delivered due to a buffer error, the communication failure mechansim is used to propagate the error; if the same failure occurs during message processing, the message processing failure mechanism is used).

In the following sections it is defined, how failures of the first three kinds are handled by epSOS. Failures of the fourth kind are handled within the documents (e.g. by nullifying fields or using specific error codes; see [epSOS D3.5.2c]).

4.6.1 Communication Failures

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.

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	HCPO that issued the original request.
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 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

4.6.2 Encoding and Consistency Failures

Encoding and consistency problems are 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.

4.6.2.1 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; see tables below for the defined values

Element name	Format	Opt.	Content
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 (see tables below) 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.

Table 10: Usage conventions for SOAP faults

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.

4.6.2.2 General Message Handling Errors

General message handling faults are detected upon receipt of a message. Usually they are not specific for a certain transaction and usually origin in weaknesses related to the implementation, configuration and operation of the epSOS NCP.

The following table lists all general message handling errors. These errors MUST be handled acc. to the epSOS SOAP error profile (see section 4.6.2.1).

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.

4.6.2.3 SOAP Message Encoding and Addressing Errors

Message encoding and addressing faults are detected upon receipt of a message or at the protocol terminator. Usually they are not specific for a certain transaction and usually origin in weaknesses related to the implementation, configuration and operation of the epSOS NCP.

The following table lists all message encoding and addressing errors. These errors MUST be handled acc. to the epSOS SOAP error profile (see section 4.6.2.1).

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 the spec)	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 error.

4.6.2.4 Security Header Encoding and Consistency Errors

Security header encoding and consistency errors are detected by the security manager component. Usually they are not specific for a certain transaction and usually origin in weaknesses related to the implementation, configuration and operation of the epSOS NCP.

The following table lists all security header related errors. These errors MUST be handled acc. to the epSOS SOAP error profile (see section 4.6.2.1).

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 HCP.
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 HCP authentication.
The patient identifier is not valid.	Sender	Unknown Patient	Both service consumer and service provider MUST write an audit trail entry. The HCP 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.
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 HCP SHOULD trigger the issuance of a new TRC assertion by NCP-B and reissue the request.

4.6.2.5 Audit Trail Considerations

In case of a general message handling error, NCP-B MUST write a full audit trail including an error section as defined in chapter 4.5.3.

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 HCP 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 section 4.5.8.3 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:

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”

5 epSOS Profiles on Assertions and Certificates

epSOS security mechanisms build upon SAML assertions and digital certificates as core secuirty objects. This chapter provides the respective epSOS security object profiles on SAML and X.509.

5.1 Cryptographic Keys and Algorithms

The following change history provides an overview of all changes to chapter 5.1 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

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 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.

5.2 HCP Identity Assertion

The following change history provides an overview of all changes to chapter 5.2 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

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.

Being part of the epSOS security architecture, the national and therefore decentralized identity management produces authentication assertions that are encoded as SAML assertions [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.

5.2.1 Generic Structure of the Identity Assertion

Figure 17 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.

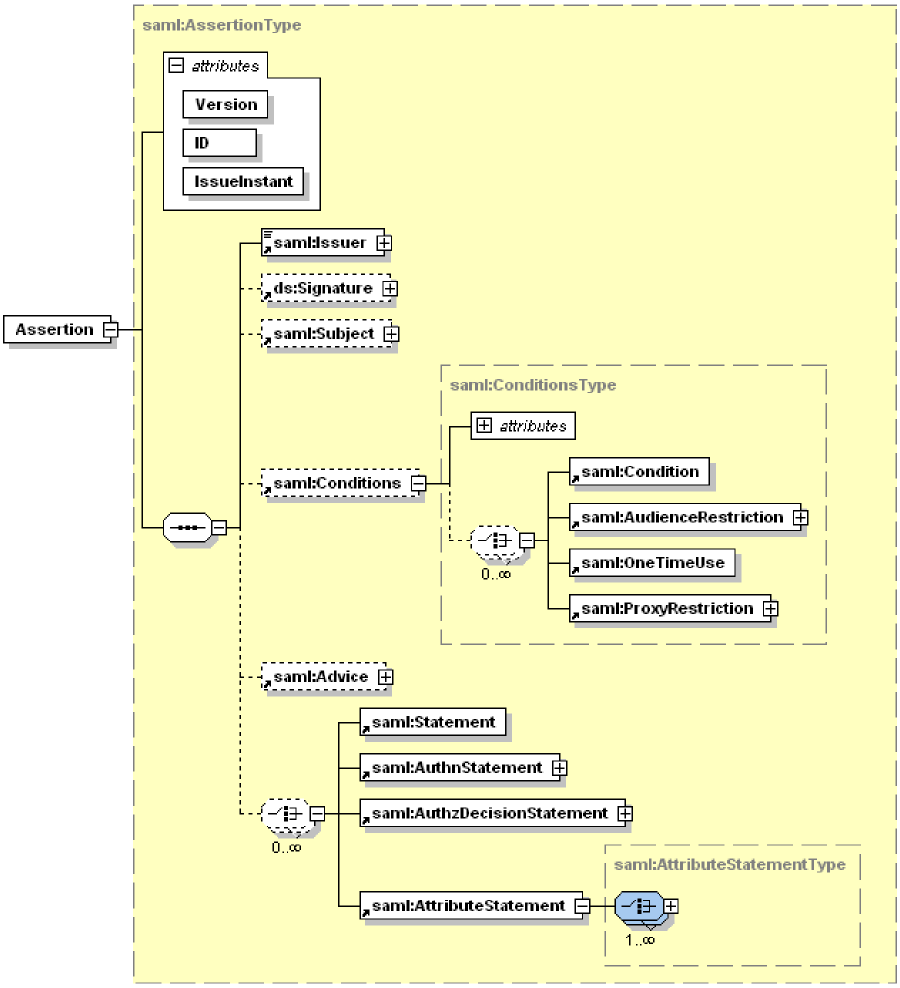


Figure 17: Identity Assertion – Top Level Elements of a SAML Assertion

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 HCP 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 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 HCP authentication method. See [OASIS SAML Authn] for a list of valid authentication methods.
AttributeStatement			R	HCP identity attributes and permissions (see sections 5.2.3 and 5.2.4)
ds:Signature			R	Enveloped XML signature of the issuer of the HCP Identity Assertion (see section 5.2.2).

5.2.2 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 section 3.1.6 of this document MUST NOT be used.
SignatureMethod	The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see section ...). 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 section ....). 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 element which contains the X.509 certificate of the assertion issuer.

5.2.3 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:2.0:subject:subject-id
Values:	Human readable name of the HCP
Type	String

Optionality:	Mandatory
Description:	This attribute MUST contain the full name of the HCP.
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 possible values.
Type:	String
Optionality:	Optional
Delegated Rights	
FriendlyName:	OnBehalfOf
Name:	urn:epsos:names:wp3.4:subject:on-behalf-of
Values:	See ASTM E1986-98 (2005). Acc. to [epSOS D3.6.2] only the ASTM structural roles “dentist”, “nurse” “pharmacist”, “physician” and “nurse midwife” MUST be used.
Type:	String
Optionality:	Mandatory if a structural role of “ancillary services” or “clinical services” is presented. For all other structural roles this attribute is optional
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 delefation to the two natural persons involved. Only valid roles as defined for HCP structural roles MUST be used. A service provider MAY decide not to accept delegated access rights by just ignoring this attribute.
Healthcare Professional Organisation	
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 section 6.2.2 of this document[26]. 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
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 HCP 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.

Pilot projects MAY agree on further attributes. Nevertheless all attributes not listed in this list MAY be ignored by the service provider.

5.2.4 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 HCP is assigned in the country of care. As these permissions can only be defined and assigned by the HCPs 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

[26] 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 [epSOS D3.6.2].

The following matrix shows which permissions MUST at least be assiged to an HCP 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

5.2.5 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+1CY … </ds:SignatureValue>
     <ds:KeyInfo>
      <ds:X509Data>
       <ds:X509Certificate>MIIIADS … </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">
   </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
 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 Hl7"
 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 Hl7 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"
    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>
```

5.3 Treatment Realtionship Confirmation Assertion

The following change history provides an overview of all changes to chapter 5.3 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

The Confirmation Assertion is a profiled SAML v2.0 assertion. It attests the existence of a treatment relationship between a patient and a HCPO and provides information about the context of a certain treatment scenario.

5.3.1 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	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 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 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 section 5.3.3)
ds:Signature	R	Signature of the issuer of the Treatment Relationship Conformation Assertion (see section 5.3.2).

5.3.2 Assertion Signature

EveryTreatment 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 section 3.1.6 of this document MUST NOT be used.
SignatureMethod	The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see section ...). 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 section ....). 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 element which contains the X.509 certificate of the assertion issuer.

5.3.3 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 requests 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.

5.3.4 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
```

```xml
       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+lCY … </ds:SignatureValue>
   <ds:KeyInfo>
    <ds:X509Data>
     <ds:X509Certificate>MIIIADS … </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: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>

 </saml:AttributeStatement>
</saml:Assertion>
```

5.3.5 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 section 4.5.3. 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	HCP 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 uses to identify active participants
Patient	R	Patient who is in a treatment relationship with the HCPO
Event Target	X	

Table 11: Contry-B NCP Audit Message Categories

5.4 epSOS Certificate Profiles

The following sections 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.

While sections 5.4.1 and 5.4.2 define general requirements on epSOS compliant certificates, the following sections specify the specifics of certain epSOS certificates:

Certificate Profile	Section	Purpose
VPN Client Gateway	5.4.3	Establishment of IPSec VPN between epSOS nodes
VPN Server Gateway	5.4.4	Establishment of IPSec VPN between epSOS nodes
Service Consumer Node Authenticity	5.4.5	Establishment of epSOS circle of trust
Service Provider Node Authenticity	5.4.6	Establishment of epSOS circle of trust
NCP Signature	5.4.7	Signatures on messages and assertions
OCSP Responder	5.4.8	OCSP Responder authenticity

Table 12: epSOS Certificate Profiles

5.4.1 Certificate Profiles - General Stipulations

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” recommendations (see chapter 5.1).

Version

Certificates to be deployed MUST be v3.

Signature algorithm

“epSOS Cryptographic Keys and Algorithms” recommendations (chapter 5.1) 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.

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]**

5.4.2 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 sections)

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.

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 sections)

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.

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.

Note: Even though AuthorityInfoAccess and CRLDistributionPoints are specified as non-mandatory extensions, one of them MUST be included in the certificate as defined above.

5.4.3 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).*

5.4.4 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).*

5.4.5 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).*

5.4.6 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).*

5.4.7 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.

ExtendedKeyUsage (non critical)

"ExtendedKeyUsage" MUST NOT be included as an extension in the certificate.

5.4.8 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)*

5.4.9 Certificate Profile: Certificate Revocation Lists

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.

The following section defines the profile (structure) of a CRL, and all CRLs issued by the CA are to be based on these guidelines. The following guidelines refer to direct CRLs.

5.4.9.1 CRL Profile - General Stipulations

CRLs MUST be Common PKI compatible.

Version
CRLs to be deployed MUST be v2.

Signature algorithm
See “epSOS Cryptographic Keys and Algorithms” recommendations (chapter 5.1).

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.

5.4.9.2 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.

6 Appendix

6.1 Coding Conventions (Normative)

The following change history provides an overview of all changes to chapter 6.1 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

6.1.1 Country Codes

Fields carrying country code values MUST be coded in accordance with [ISO 3166-1] Alpha 2 codes. The following exceptions apply:

- For United Kingdom the country codes “GB” and “UK” are allowed.
- For Greece the country codes “GR” and “EL” are allowed.

6.2 epSOS Identifiers

The following change history provides an overview of all changes to chapter 6.2 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

6.2.1 epSOS WP3.4 URNs

Recently there are no URNs defined for epSOS WP3.4.

6.2.2 epSOS WP3.4 OIDS

For epSOS WP3.4 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

6.3 Examples (Informative)

The following change history provides an overview of all changes to chapter 6.3 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

6.3.1 epSOS Full Request Message

This example message will be added after the expert review when the spec and the WSDLs are stable.

6.3.2 epSOS Full Response Message

This example message will be added after the expert review when the spec and the WSDLs are stable.

6.3.3 epSOS NCP-Service Status List

.....

```
<?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">
          <tsl:StreetAddress>...</tsl:StreetAddress>
          <tsl:Locality>...</tsl:Locality>
          <tsl:PostalCode>...</tsl:PostalCode>
          <tsl:CountryName>XX</tsl:CountryName>
        </tsl:PostalAddress>
      </tsl:PostalAddresses>
      <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>
         <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:TSPInformationURI>
            <tsl:URI xml:lang="xx"> http://www.ncp.epsos.xx/docs/</tsl:URI>
         </tsl:TSPInformationURI>
      </tsl:TSPInformation>
      <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>
                  <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-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:ServiceTypeIdentifier>
         http://uri.epsos.eu/TrstSvc/Svctype/PatientIdentificationService
      </tsl:ServiceTypeIdentifier
      <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
      </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>
              <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:TSPInformation>
        <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:TSPInformationURI>
          <tsl:URI xml:lang="xx"> http://www.ncp.epsos.xx/docs/</tsl:URI>
        </tsl:TSPInformationURI>
```

```
         </tsl:TSPInformation>
         <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-B 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>
                     <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="....">
   ....
```

```
</dsig:Signature>
</tsl:TrustServiceStatusList>
```

6.4 WSDLs

The following change history provides an overview of all changes to chapter 6.4 that have been done since v1.00 of this document.

V	Category	Change Request	Change in Document

This section lists the WSDLs for the epSOS messages. The schemas for the messages and contained data types are included with a ZIP-File that is distributed together with this document.

6.4.1 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

    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"/>
        </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>
</wsdl:definitions>
```

6.4.2 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>
       <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>
```

6.4.3 IHE XDR Document Recipent

```
<?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>
   <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>
```

6.4.4 IHE XDR Metadata Update Delete

```
<?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">
                    <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>
```

7 References

Note : The references will be reviewed and completed in parallel with the quality review. Please do not comment on this list.

[BSI TR-3116] Bundesamt für Sicherheit in der Informationstechnik: BSI - Technische Richtlinie 03116 für die eCard-Projekte der Bundesregierung. Version 3.0. April 2009.

[DICOM Sup95] Digital Imaging and Communications in Medicine (DI-COM): Supplement 95 – Audit Trail Messages. 18. June 2004.

[Ecrypt-II D.SPA.7] Ecrypt-II NoE: ECRYPT2 Yearly Report on Algorithms and Keysizes (2008-2009). July 2009.
http://www.ecrypt.eu.org/documents/D.SPA.7.pdf

[epSOS ConceptPaper] Z. Kolitsi, P. Wilson (Eds.): epSOS Trusted Domians Consolidation of Concepts. Version Final 0.1. June 2009.

[epSOS D2.1.1] Z. Kolitsi, G. Pangalos (Eds.): Legal and Regulatory Constraints on epSOS Design. Final Draft Version. January 2009.

[epSOS D3.1.2] M. Bonilla, M. J. Pina (Eds.): Final definition of functional service requirements – ePrescription. Version 1.0. September 2009.

[epSOS D3.2.2] C. Vaquerizo (Ed.): Final definition of functional service requirements – Patient Summary. Version 0.6. June 2010.

[epSOS D3.3.2] P. Ruestchmann, G. de Béjarry, S. Lotti (Eds.): System Technical Specification. Version 1.4. April 2010.

[epSOS D3.3.3] D. Ambroise, A. Janeczek, P. Ruestchmann, G. de Béjarry (Eds.): epSOS Interoperability Framework. Version 2.3. April 2010.

[epSOS D3.5.2] A. Estelrich (Ed.): Semantic Service Definition. Version 0.0.6. May 2010

[epSOS D3.5.2C] A. Estelrich (Ed.): Semantic Services Appendix C – Pivot Documents Specifications. Version 0.0.6. May 2010

[epSOS D3.6.2] G. Heider, M. Hurch (Eds.): epSOS Identity Management. Version 1.1. April 2010

[epSOS D3.7.2] E. Albertini, G. Orsi (Eds.): epSOS Security Services Specification – Master Document. Version 0.4. March 2010

[epSOS D3.7.2-II] E. Albertini, G. Orsi (Eds.): epSOS Security Services Specification – Security Services. Version 0.4.21. May 2010

[FNISA CryptMech] Secrétariat général de la défense nationale: Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard. Version 1.1. December 2006.

[HITSP C80 2.0] Healthcare Information Technology Standard Panel : HITSP C80 - Clinical Document and Message Terminology Component v2.0. January 2010.
http://www.hitsp.org/Handlers/HitspFileServer.aspx?
FileGuid=886331bd-2eba-4ded-a1ed-24b35ecebb62

[HL7 Datatypes] ....

[HL7 WS SOAP] HL7 Web Service transport specification SOAP binding

[IHE AC WP] IHE International: IHE White Paper on Access Control. September 2009

[IHE ITI TF-1] IHE International: IHE IT Infrastructure (ITI) Technical Framework. Volume 1: Integration Profiles. August 2009

[IHE ITI TF-2a] IHE International: IHE IT Infrastructure (ITI) Technical Framework. Volume 2a: Transactions. August 2009

[IHE ITI TF-2b] IHE International: IHE IT Infrastructure (ITI) Technical Framework. Volume 2b: Transactions. August 2009

[IHE ITI TF-2x] IHE International: IHE IT Infrastructure (ITI) Technical Framework. Volume 2x: Appendices and Glossary. August 2009

[IHE ITI TF-3] IHE International: IHE IT Infrastructure (ITI) Technical Framework. Volume 3 – Document Content Profiles. October 2008

[IHE PCC TF1] IHE International: IHE Patient Care Coordination (PCC) Technical Framework. Volume 1: Integration Profiles. August 2008

[IHE PCC TF2] IHE International: IHE Patient Care Coordination (PCC) Technical Framework. Volume 2: Transactions. August 2008

[IHE PIX/PDQ v3] IHE International: Patient Identifier Cross-Reference (PIX) and Patient Demographic Query (PDQ) HL7 v3. August 2009

[IHE SVS] IHE International: IHE IT Infrastructure (ITI) Technical Framework Supplement 2008-2009. Sharing Value Sets (SVS). August 2008.

[IHE XCPD] IHE International: Cross-Community Patient Discovery (XCPD). August 2009.

[IHE XUA++] ....

[ISO OID] ISO/IEC 9834-1:2005: Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree.

[ISO/IEC 9834/1] ISO/IEC 9834-1:2005: Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree. 2005.

[NHIN PID] US Nationwide Health Information Network: NHIN Draft Production Service Interface Specifications: Patient Discovery. Version 0.9. September 2009.

[NHIN QDOC] US Nationwide Health Information Network: NHIN Draft Production Service Interface Specifications: Query for Documents. Version 1.6.10. June 2009.

[NIST SP800.57/1] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid (Eds.): NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General. March 2007.

[NTPv4Draft] D. Mills: Network Time Protocol Version 4 Protocol And Algorithms Specification. September 2008. http://tools.ietf.org/html/draft-ietf-ntp-ntpv4-proto-11

[RFC 1305] D. Mills: Network Time Protocol (Version 3) Specification, Implementation and Analysis. March 1992.

[RFC1778] T. Howes, S. Kille, W. Yeong, C. Robbes: The String Representation of Standard Attribute Syntaxes (RFC 1778). March 1995.

[RFC 2119] Bradner, S.: Key words for use in RFCs to Indicate Requirement Levels; Harvard University, Boston, Massachusetts, 1997.

[RFC 2246] T. Dierks, C. Allen: The TLS Protocol. Version 1.0. January 1999.

[RFC 2616] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee: Hypertext Transfer Protocol - HTTP/1.1. June 1999.

[RFC 2818] E. Rescorla: HTTP over TLS. May 2000.

[RFC 3061] M. Mealling: A URN Namespace of Object Identifiers. February 2001.

[RFC 3369] R. Housley: Cryptographic Message Syntax (CMS). August 2002.

[RFC 3881] Marshall, G.: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications. Version 1.0. September 2004.

[RFC 3986] T. Berners-Lee, R. Fielding, L. Masinter: Uniform Resource Identifier (URI): Generic Syntax. January 2005.

[RFC 4330] D. Mills: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI. January 2006.

[RFC 4346] T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol. Version 1.1. April 2006.

[RFC 4511] J. Sermersheim (Ed.): Lightweight Directory Access Protocol (LDAP): The Protocol. June 2006.

[RFC 4634] D. Eastlake, T. Hansen: US Secure Hash Algorithms (SHA and HMAC-SHA). July 2006.

[RFC 5246] T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol. Version 1.2. August 2008

[SAML 2.0] S. Cantor, J. Kemp, R Philpott, E. Maler: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. March 2005.

[STORK] eID STORK Project; http://www.eId-stork.eu/

[W3C WSDL 1.1] E. Christensen, F. Curbera, G. Meredith, S Weerawarana: Web Services Description Language (WSDL). Version 1.1. March 2001

[WSI BP 1.1] Web Services Interoperability Organization: WS-I Basic Profile. Version 1.1. August 2004.

[WSI BP 2.0] Web Services Interoperability Organization: WS-I Basic Profile. Version 2.0. Working Group Draft. October 2007.

[WSI SBP 1.1] Web Services Interoperability Organization: WS-I Basic Security Profile. Version 1.1. January 2010.

[WS Trust] A. Nadalin, et al.: WS-Trust. Version 1.3. March 2007. http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf

[XML-EXC 1.0] J. Boyer et al: Exclusive XML Canonicalization. Version 1.0. W3C Recommendation, July 2002. http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/

[XML_Schema-1.1] D. Peterson et al: XML Schema. Version 1.1, W3C Recommendation, February 2006. http://www.w3.org/XML/Schema

[XMLDSig BP] F. Hirsch, P. Datta: XML Signature Best Practices. W3C Working Draft. Februray 2010. http://www.w3.org/TR/xmldsig-bestpractices/

8 Abbreviations

ATNA	Audit Trail and Node Authentication (IHE Profile)
B2B	Business to Business (communication paradigm)
CoT	Circle of Trust
CRL	Certificate Revocation List
E2E	End to End (security services)
epSOS	Smart Open Services for European Patients
HCP	Healthcare Professional (e. g. physician, pharmacist, nurse)
HCPO	Healthcare Professional Organisation
HL7	Health Level 7 (International Standardisation Organisation)
IHE	Integrating the Healthcare Enterprise
MPI	Master Patient Index
NCP	National Contact Point
NSL	NCP Trusted Service List
NTP	Network Time Protocol [RFC 1305]
OID	ISO Object Identifier
OMG	Object Management Group (International Standardisation Organisation)
PKI	Public Key Infrastructure
PoC	Point of Care
RST/RSTR	Request Security Token and Request Security Token Response Messages as defined in [WS Trust 1.3]
SAML	Security Assertion Markup Language
SOAP	XML protocol for exchanging messages between web services
STORK	EC funded project for the establishment of a European eID Interoperability Platform
STS	Security Token Service
TLS	Transport Layer Security (Protocol)
TSL	Trusted Service List
URI	Uniform Resource Identifier [RFC 3986]
URL	Uniform Resource Locator [RFC 3986]
URN	Uniform Resource Name [RFC 2141]
WS*	Collection of Web Services Specifications (WS Trust, WS SecureConversation, etc.)
WSC	WebService Consumer
WSP	WebService Provider
WSDL	Web Service Description Language