



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	28/04/2010



Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of
Patient Summary and electronic Prescription

D3.3.2 Final epSOS System Technical Specification

D3.3.2_v1.4

WORK PACKAGE	WP3.3
DOCUMENT NAME	D3.3.2_v1.4
SHORT NAME	D3.3.2
DOCUMENT VERSION	1.4



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	28/04/2010



D3.3.2_v1.4	Document Short name: D3.3.2
	Version: 1.4
WP3.3: System architecture	Date: 30/04/2010

COVER AND CONTROL PAGE OF DOCUMENT

Document name:	D3.3.2 Final epSOS System Technical Specification
Document Short name:	D3.3.2
Distribution level	Public
Status	Final
Author(s):	& Gil de Béjarry
Organization:	ASIP SANTE

Dissemination level: PU = Public, PP = Restricted to other programme participants, RE = Restricted to a group specified by the consortium, CO = Confidential, only for members of the consortium.

ABSTRACT

D3.3.2 is the second deliverable for WP3.3 epSOS architecture as stated in the Annex 1 (Grant Agreement). It expands the D3.3.1 deliverable mainly with the technology view.

CHANGE HISTORY

Version	Date	Status Changes	From	Details	Review
V1.0	01/12/09	Draft	ASIP Santé, LOMBARDY	Version submitted for Internal Review	WP3.3 members
V1	17/12/09	Draft	ASIP Santé	Version submitted for Quality Review	WP3.8, WP3.9, NHS, IZIP, ELGA, FHGISST, THESS, LOMBARDY, ANDA
V1.1	20/01/10	Final	ASIP Santé	Version issued after Quality Review	NHS, IZIP, ELGA, FHGISST, THESS, LOMBARDY, ANDA, ESNA
V1.2	25/01/10	Final	ASIP Santé	Revised version	ASIP Santé
V1.2.1	29/01/10	Final	ASIP Santé	Final adjustments with issued D3.x.2	ASIP Santé
V1.3	08/04/10	Final	ASIP Santé	Solutions from Berlin open Issues & WP 3.x alignments	NHS, IZIP, ELGA, FHGISST, THESS, LOMBARDY, ESNA
V1.4	30/04/10	Final	ASIP Santé	Version issued after TMP comments	ASIP Santé



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture

Date: 30/04/2010

REFERRING DOCUMENTS

Date	Type	Description	Version	Origin	Document
2008-06-30	pdf	Annex I – “Description of Work”	-	EMP/S.O. S. LSP- eHealth team	epSOS_Grant_Agreement_Annex-I
2009-05-21	doc	epSOS Trusted Domain(s): Consolidation of Concepts	0.3	WP2.1	epSOS Concepts paper v3
2009-12-11	pdf	D3.2.2 Final definition of functional service requirements- Patient Summary	0.4	WP 3.2	Draft_D3.2.2_v0.4.pdf
2009-09-07	doc	D3.1.2 Final definition of functional service requirements – ePrescription	1.0	WP 3.1	D3.1.2 epSOS WP 3 1_tc-v1.doc
2009-04-01	doc	D3.4.2 Final common components specifications	0.20.0	WP3.4	WP34_D342_FHGISST_V-IHE- 0.20.doc
2009-12-11	doc	D3.5.2 epSOS Pivot Documents Specifications	0.0.2	WP3.5	D3.5.2_epSOS_WP_3.5_v0.0.2
2009-12-22	doc	D3.6.2 Identity Management	1.0	WP3.6	WP36_D362 Draft identity management V1.0
2010-01-14	pdf	D3.7.2 Security Services D3.7.2 Security Services section II D3.7.2 Security Policy section I	0.2 0.2 0.6	WP3.7	WP3.7_D3.7.2_SECTION_II_Securi ty_Services_V02.pdf WP3.7_D3.7.2_SECTION_I_Securit y_Policy_V06.pdf WP3.7_D3.7.2_Security_Services_ V02.pdf
2009-08-20	pdf	epSOS Architecture: Consolidated Work	0.4	WP3.3	epSOS_Archi_Consolidated_Work_ V0.4
2009-05-22	doc	Status and Requests for Discussions	0.3	WP3.3, WP3.4	WP3.3-4_Stauts_May09_v03.doc
2010-04-30	doc	Common Components for the NCP	0.52	WP 3.8,WP 3.9	JWG_NCP_Architecture_HLDD.doc



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010
WP3.3: System architecture		

WORKSHOPS (Face to Face)		
Date	Location	Conclusion document
2009-03-17	Brussels	090317_02_epSOS-layers_and_transactions-rough_cut.ppt
2009-04-17	Milan	Presentation and Conclusions WP3.3-4 KickOff Milano v03.ppt
2009-05-04	Paris	WP3.3-x_Workshop_Paris090504_final.ppt
2009-05-28	Paris	WP3.3-4_Workshop_Paris090528_v0.2.ppt
2009-09-11	Berlin	WP3.4_11_06_2009_Minutes_v01.doc
2009-07-30	Vienna	WP3.3-4__Workshop_Vienna090730_v0.3.ppt
2009-07-31	Vienna	WP3.4_Workshop_Vienna090731_v0.2.ppt
2009-09-11	Berlin	WP3.4_11_06_2009_Minutes_v01.doc
2009-10-23	Paris	WP3.3-4_workshop_Paris091023.ppt
2010-02-17	Berlin	TPM_taskforce_OpenIssues_100319.xls



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

Table of content

- 1. Executive Summary 15**
- 2. Introduction 18**
- 3. Context & Methodology 20**
 - 3.1 Methodology and approach 20**
 - 3.2 epSOS requirements derived from the Use Cases 23**
 - 3.2.1 epSOS Use Cases 23**
 - 3.2.2 Use cases assumptions related to HCP identification, authentication and authorisation 25**
 - 3.2.3 Use cases assumptions related to patient identification and authentication . 26**
 - 3.2.4 Use cases assumptions related to patient consent 27**
 - 3.2.5 Supplementary specification related to trust between countries 29**
 - 3.2.6 Supplementary specification related to data exchange/access 29**
 - 3.2.7 Supplementary specification related to medical data transformation 30**
 - 3.2.8 epSOS Core Business Blocks derived from FR/NFRs 30**
 - 3.3 Basic Concepts and Principles 34**
- 4. Business View 41**
 - 4.1 epSOS Information Model 41**
 - 4.1.1 Actors, Roles and Objects 41**
 - 4.1.2 Relationships between actors & objects: Information Model 42**
 - 4.2 epSOS processes 43**
 - 4.2.1 Establishment of a secure context between 2 NCPs 43**
 - 4.2.2 Medical data exchange & handling 46**



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture

Date: 30/04/2010

4.2.3 **Groups of epSOS processes..... 48**

4.2.4 **Description of the flow of control 48**

4.2.5 **Exception Handling..... 59**

4.3 **Synthesis: Business view..... 61**

5. **Information System View 63**

5.1 **From Business view to epSOS Information System view..... 63**

5.2 **Descriptions of the epSOS services..... 67**

5.2.1 **Trust – Audit Services 67**

5.2.1.1 **Internal & External Services 69**

5.2.1.2 **Internal services 70**

5.2.1.3 **External services 70**

5.2.2 **Data Exchanges – Data Transformation Services 71**

5.2.2.1 **Internal & External Services 71**

5.2.2.2 **Internal services 71**

5.2.2.3 **External services 71**

5.2.3 **epSOS support services..... 71**

5.2.3.1 **National Contact Point Routing Table..... 72**

5.2.3.2 **Trusted Certificates 72**

5.2.3.3 **Taxonomy for the epSOS pivot format central function..... 72**

5.2.3.4 **Traits Handshake central function 73**

5.3 **NCP considerations 73**

5.3.1 **NCP Interface to national domain 75**

5.3.2 **NCP Interface to epSOS domain 76**

5.4 **Security considerations..... 76**



D3.3.2_v1.4

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

WP3.3: System architecture

5.5	Information Objects	77
5.5.1	Health Care Professional (HCP).....	79
5.5.1.1	Healthcare Professional Address.....	79
5.5.1.2	Health Care Professional Organization (HCPO).....	79
5.5.2	Patient	79
5.5.3	Patient Summary (PS).....	80
5.5.3.1	Medication Summary.....	81
5.5.4	ePrescription (eP).....	81
5.5.5	eDispense	83
6.	Technology View.....	85
6.1	From Information System view to Technology view	85
6.2	epSOS platform	86
6.2.1	Foreword.....	86
6.2.2	epSOS Domains	87
6.2.2.1	epSOS communication layer	87
6.2.2.2	Business Layer	88
6.2.2.3	National communication layer	88
6.3	epSOS Technical Architecture	88
6.3.1	Introduction	88
6.3.2	Service Architecture	89
6.4	Composite Structure.....	92
6.4.1	Components Description.....	93
6.4.1.1	The National Communication layer.....	93
6.4.1.2	The Business Layer.....	93



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

- 6.4.1.3 The National Communication Layer..... 94**
- 6.4.1.4 The Platform layer 94**
- 6.4.2 Components Description..... 95**
- 6.4.2.1 Inbound Protocol Terminator 96**
- 6.4.2.2 Outbound Protocol Terminator 97**
- 6.4.2.3 Workflow Manager..... 98**
- 6.4.2.4 RoutingManager 100**
- 6.4.2.5 Transformation Manager..... 101**
- 6.4.2.6 Terminology Access Manager 105**
- 6.4.2.6.1 Interaction diagrams for semantic..... 109**
- 6.4.2.7 Security Manager..... 111**
- 6.4.2.8 AuditTrail..... 113**
- 6.4.2.9 Routing Manager 114**
- 6.4.2.10 Configuration And Monitoring Manager..... 115**
- 6.4.2.11 NationalConnector..... 116**
- 6.4.3 Components Communication workflow..... 118**
- 6.4.3.1 Patient Identification 118**
- 6.4.3.2 Data Exchange (PS & EP)..... 120**
- 6.4.3.3 Notification..... 123**
- 6.5 Interfaces 126**
- 6.5.1 epSOS Gateway Interfaces..... 126**
- 6.5.1.1 IdentificationService..... 126**
- 6.5.1.2 PatientService (Patient Summary) 128**
- 6.5.1.3 epSOS Order OrderService (ePrescription)..... 130**



D3.3.2_v1.4

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

WP3.3: System architecture

6.5.1.4	DispensationService	132
6.5.1.5	ConsentService.....	135
6.6	Security Architecture	138
6.6.1	Trusted Federation of NCPs	138
6.6.1.1	NCP certificates	139
6.6.2	Message exchange infrastructure	139
6.6.3	Upper Layer (Iso 7).....	140
6.6.3.1	Transmission of authenticated HCP	141
6.6.3.2	Common message format.....	141
6.6.3.3	Signature on message.....	141
6.6.4	TCP Message Layer (Iso 4).....	142
6.6.5	IPsec VPN Network Layer (Iso 3)	142
6.6.6	Physical Infrastructure Layer (Iso1)	142
6.6.7	Regarding the use of Certificates and PKI (Security Annex II of D3.7.2).....	142
6.6.8	Regarding Node authentication	143
6.6.9	Regarding SAML Assertions.....	143
6.6.10	Regarding SOAP faults	144
6.6.10.1	Message processing fault	144
6.6.10.2	Business processing / request faults.....	144
6.6.10.3	Clinical processing / content faults.....	145
6.6.11	Security zone from WP 3.7.....	145
6.6.12	Session context	146
6.6.13	Adopted Standards.....	147
6.7	Profile and Transaction Mapping.....	150



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

- 7. Terminology and Glossary..... 151**
- 7.1 Wording conventions..... 151**
- 7.2 epSOS Glossary 151**
- 8. Annexes 159**
- 8.1 Contact List..... 159**
- 8.2 Previous technical analysis..... 159**


	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

Table of Figures

Figure 1: epSOS “overall” picture	1
Figure 2: Mutual circle of between NCPs	18
Figure 3: Architecture Building Methodology.....	20
Figure 4: Classes of documents for PD3 Specification and Implementation.....	21
Figure 5: FR & NFR consolidated view	34
Figure 6: epSOS Information Model.....	42
Figure 7: epSOS Core Business Processes	43
Figure 8: Secure Context Establishment.....	44
Figure 9: Data Exchange and Handling	46
Figure 10: Processes supporting core building blocks	48
Figure 11: epSOS HCP Identification & Authentication	49
Figure 12: Patient identification.....	51
Figure 13: Treatment Relationship Confirmation.....	53
Figure 14: Data retrieval	55
Figure 15: Semantic Services – NCP-A Data Transformation.....	57
Figure 16: Semantic Services – NCP-B Data Transformation.....	57
Figure 17: Send Notification	58
Figure 18: The epSOS services at business level.....	61
Figure 19: epSOS Business View.....	62
Figure 20: epSOS NCP basic structure	64
Figure 21: epSOS logical view.....	65
Figure 22: Services regarding national and epSOS domains.....	66
Figure 23: Services”zoning” Overview	67
Figure 24: Security Context (“Trust Chain”)	68
Figure 25: High Level Architecture of a epSOS NCP	74



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

Figure 26: Detailed Composition of NCP components 75

Figure 27: Schematic representation of the Data Objects and their relations 78

Figure 28: Life cycle of the Patient Summary..... 81

Figure 29: Suggested Lifecycle of an ePrescription 83

Figure 30: epSOS domains view 87

Figure 31 : Core epSOS technical service architecture..... 90

Figure 32: Composite Structure of the NCP Gateway Implementation..... 92

Figure 33: Inbound Protocol Terminator 96

Figure 34: Outbound Protocol Terminator..... 97

Figure 35: Workflow Manager..... 98

Figure 36: Routing Manager 100

Figure 37: Transformation Manager..... 101

Figure 38: Terminology Access Manager..... 106

Figure 39: EpSOS CDA traduction..... 109

Figure 40: Transformation to epSOS CDA..... 110

Figure 41: Security Manager..... 111

Figure 42 Audit Component..... 113

Figure 43: Routing Manager 114

Figure 44: Configuration and Monitoring..... 115

Figure 45 National Connector 116

Figure 46: PatientIdentification 118

Figure 47: Patient data workflow..... 120

Figure 48: Notification Workflow 123

Figure 49: Identification Service..... 126

Figure 50: Patient Service 128

Figure 51: Order Service ePrescription..... 130



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

Figure 52: Dispensation Service 132

Figure 53: Consent Service 135

Figure 54: Message exchange layers 140

Figure 55: Soap faults..... 144

Figure 56: End-to-End security and Trust Zones (WP3.7)..... 145

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

1. Executive Summary

The goal of epSOS is to demonstrate that pan-European health data exchange can be effective in seamless manner for the Health Care Professional (HCP). Two basic pillars have to be kept in mind: existing national healthcare infrastructures / legislation remain unchanged; trust among Member State (MS) is based on contracts and agreed policies.

The task of the epSOS Architecture is to give the necessary guidelines for implementing the Large Scale Pilot of epSOS and is founded on the results of all Project Domain 3 Work Packages and the results of WP2.1 Legal Team.

A brief synthesis of the principles that drive the architecture is:

1. all epSOS communications are done via gateways and thus have a Business to Business communication model
2. epSOS must not alter existing medical data in the national systems,
3. records of all exchanges within epSOS are required and stored,
4. business transactions are designed separately of security but rely on the provision of a security context ("Circle of Trust"),
5. the architecture and its services must be extensible to cover possible new supplementary specification in further implementations of epSOS pilots.
6. a Service Orientated Architecture (SOA) is suitable to provide a loosely-integrated suite of services that can be used within the multiple business domains covered by MS in epSOS.
7. the opportunity to implement a common components solution that fits MS needs to ease medical European exchanges.

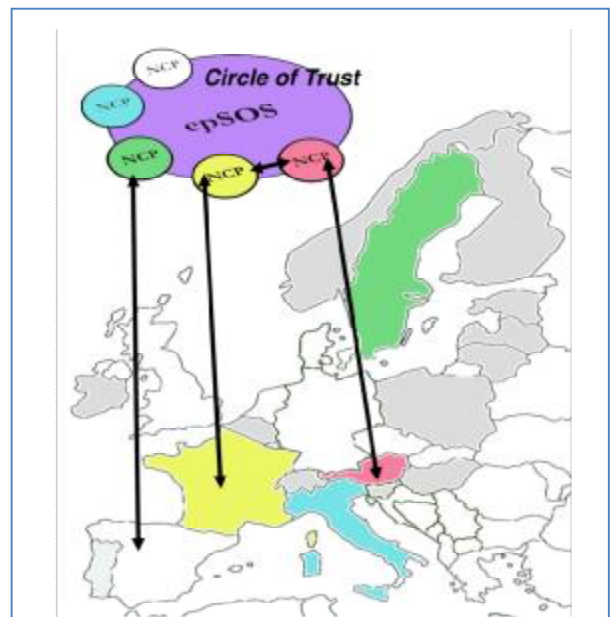



Figure 1: epSOS "overall" picture

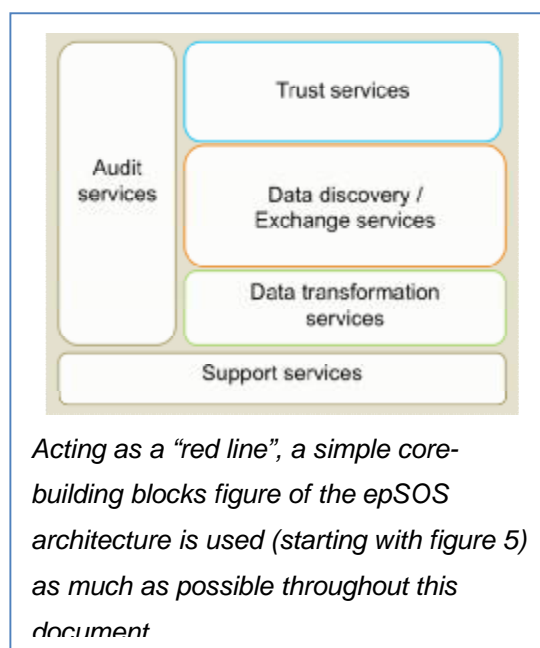
A circle of trust is build between NCP in the "epSOS abstract space", the only way a MS can exchange with another MS.


	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

It is important to note that the full technical architecture is based on the results of the following technical Work Packages:

- *WP3.3 Architecture*, which provides a flexible architecture, mapping of functional and non-functional requirements from WP2.1/3.1/3.2, data model and specifications for the epSOS services blocks (this document).
- *WP3.4 Common Components*, which subsequently derives and designs common components (epSOS Profiles, technical and policies processes, technology specifications (D3.4.2).
- *WP3.5 Semantic Services*, which provides the payload and the metadata for the Patient Summary, ePrescription and eDispense documents (D3.5.2).
- *WP3.6 Identity Management*, which provides specifications for identity management, authentication, authorisation and audit topics, including Patient Consent (D3.6.2).
- *WP3.7 Security Services*, which defines the security system in regard to confidentiality, integrity, availability and liability of data (D3.7.2).
- *WP 3.8 JWG which defines common components implementation and deployment.*

In this document (D3.3.2), the epSOS architecture is partitioned into the three classical viewpoints: Business View, Information System View and Technology View. This approach, inter alia, supports a sufficient level of abstraction useful to architect a system of heterogeneous healthcare national infrastructure. Furthermore this level of heterogeneity makes epSOS a typical field for a Service Oriented Architecture (SOA) style. In this context the architecture must be abstracted from the complexity-characteristic-platform of underlying systems (loose coupling principle). The specific



	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

technical implementation of a service should be hidden for the consumer. The components of an epSOS National Contact Point (NCP) can be viewed like a logical “wrapper” of the different National Infrastructures.

The basic blocks of the architecture (epSOS profiles) are built upon three main operations: *Query*, *Retrieve* and *Notify*. Those operations, which are fully described in D3.4.2, are the unitary blocks needed to perform the exchanges of data between MS in the epSOS context.

This document (D3.3.2) covers the most technical part (technology view), giving guidelines for a pilot implementation of an epSOS NCP. D3.3.2 is meant to embrace those works in the most comprehensive manner without repeating those results unnecessarily. Hence, whenever possible, references have been made to the deliverables of WP3.4 to WP3.7.

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

2. Introduction

This deliverable is the second draft for epSOS Architecture. The main goal is to provide an appropriate view for epSOS, detailing functionalities, components, interfaces and infrastructures, from which technical realizations result. This document is the final deliverable as expressed in Annex I. Chapter 5 and 6 gives the more technical specs about NCP-NCP.

epSOS has the objective of improving health care services for European citizens therefore its use must remain simple for both patient¹ and health care professionals. Such a large scale pilot will increase the value of pan-European health data exchange providing new feeds for existing processes and infrastructures. The challenge is to demonstrate that pan-European health data exchange can be done in a regularly and easily manner without changing existing national healthcare infrastructures and legislations, within a trust framework (contracts and agreed policies) among Member States.

EpSOS architecture is to provide PS and eP cross-border interoperability. EpSOS is implemented as a set of interacting National Contact Points² (further, simply “NCPs”) built on top of Web technology. Each NCP agrees to exchange medical data under a mutual circle of trust as shown on figure below:

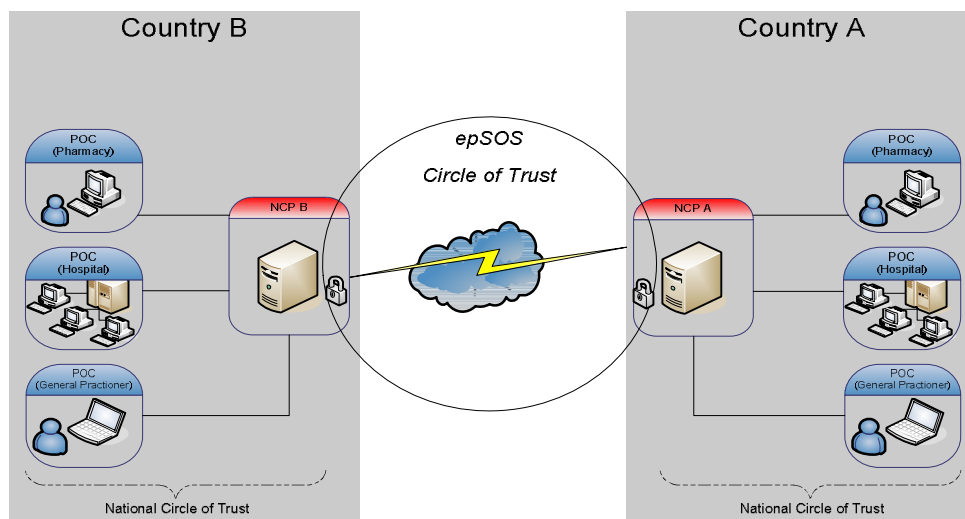



Figure 2: Mutual circle of between NCPs

¹ Patient is considered as adult and minors are to be handled in the same way as adult in 2011 epSOS pilot

² Section 9.2 (epSOS Glossary) gives the exact definition for “NCP”.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

The number of NCPs is first limited to the countries involved in the pilot but will increase in the future as new Member States (MS) enter epSOS. Therefore the architecture must be scalable in respect to the number of participating MS and the number of supported use cases.

The epSOS pilots can be considered as a project for communication between National Infrastructures of Member States and not directly between HCP(O)³ or a patient and an HCP(O).

The epSOS Architecture is the technical and conceptual translation of those main sources:


1. the Use Cases (UC) from the Initial Scope Document,
2. the functional and non functional requirements issued by WP3.1 and WP3.2, deduced from the UCs,
3. the security requirements from WP3.7,
4. the identity management requirements from WP3.6,
5. the semantic interoperability services from WP3.5,
6. the common components from WP3.4,
7. the common implementation from JWG WP3.8.

In this context, WP3.3 acts as an assembly line for other PD3 work packages, each involved in essential and specific inputs for the architecture.

This document firstly focuses on the key business specifications that help to drive the design work on the architecture. It, then, states the basic concepts and principles that were derived from the analysis of the use cases requirements. On this basis, the core content of this deliverable is given through different views of the architecture that will be explained in the next chapters:

1. A Business View
2. An Information System View
3. A Technology View

³ In this document, no distinction between the Health Care Professional (HCP) and the HCP Organization Institution (HCPO) will be made, please refer to WP3.2 for further information about HCP(O)

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

3. Context & Methodology

This chapter gives an overview of the methodology followed in order to provide the epSOS architecture, focuses on the key specification derived from the results of WP3.1 and WP3.2. It then concludes on the basic principles that drive the architecture design.

3.1 Methodology and approach

The key features of the methodology followed (figure 3) are straightforward and have adapted itself to the various debates running around key functional issues such as Multiple or Single Patient Summary or patient consent. The participants of WP3.3 and WP3.4 came back systematically to the roots of the Use Cases and focused on the feasibility of the Large Scale Pilot (LSP).

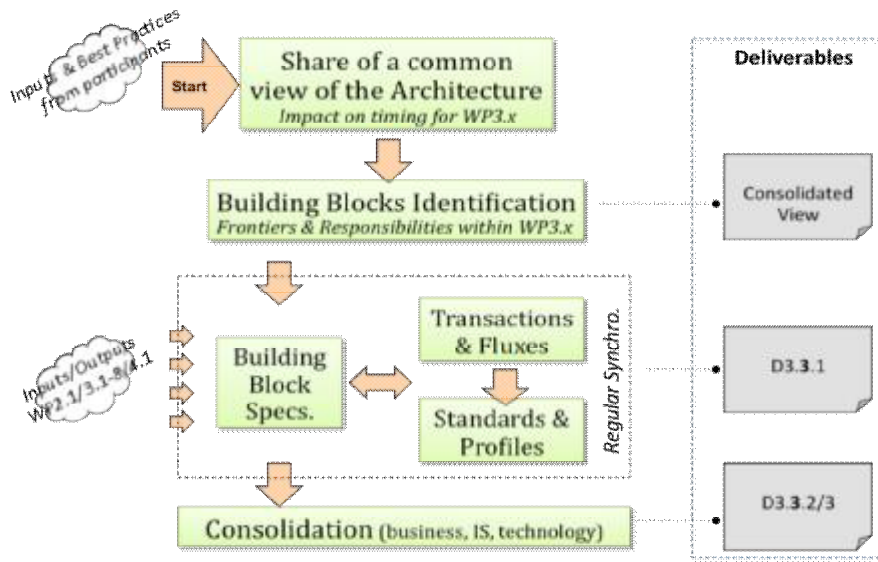



Figure 3: Architecture Building Methodology

Considering this approach, a joint work with WP3.4 “Common Components” has been engaged from the very beginning in order to produce cross-over reflexions and practical results.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

In order to prepare this deliverable, a work plan has been drawn (figure 4). This map was used as a tool that helped the work package to proceed in the assembly of the various reflexions.

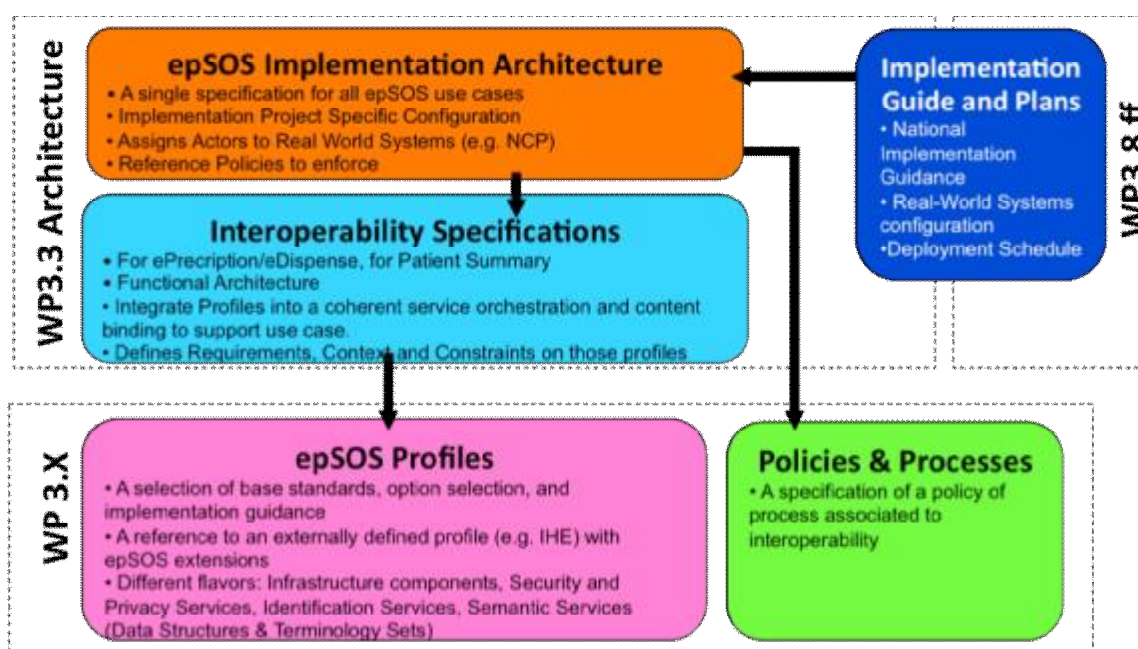


Figure 4: Classes of documents for PD3 Specification and Implementation

Eventually, the above five classes, from the less epSOS specifics (bottom of the figure) to the LSP related implementation architecture (top), found their way into the actual structure for the architecture (Business, IS and Technology view):

§ in chapters “Information System View” and “Technology View” of this document,

§ in D3.4.2 Common Components deliverable,

§ in D3.3.3 Interoperability Framework.

Note on epSOS profiles: The epSOS profiles act as basic specification blocks manipulated within the epSOS architecture. It has been the task of WP3.4 to specify each of these profiles based on the joint work of the Architecture and Common Components. Doing so, each profile has been kept as independent as possible from other profiles in order to allow the most flexible grouping and the easier reuse. Consistent “Profile Groups” have been composed (each group contains a number of epSOS Profiles, see chapter “Technology View” for details and how they are bound to the overall architecture):



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

As mentioned in the Introduction, the architecture is partitioned into the three classical views derived from TOGAF⁴:

§ *Business Architecture (Business view)*, which describes a Computationally Independent Model referring to the epSOS domain of interest without technical considerations. This view is devoted to identification of the actors, data objects and relevant processes for the epSOS system to operate from a business point of view (HCP(O)/Patient).

§ *Information System Architecture (IS view)*, which describes a Platform Independent Model and looks at the system in a computational complete

way but without any implementation specific detail. This view is principally devoted to the identification of epSOS services - and their collaboration - derived from the processes (ref. to Business view). Components and service interface are described as well.

§ *Technology Architecture (Technology view)*, which describes a Platform Specific Model (i.e. a general webservices stack, not specific to a programming language/technology) that maps and specifies the Information System view onto specific technology options for the epSOS system. This view refers to the epSOS Profiles and their most technical part.

Consideration on modelling format within this document:


The Unified Modeling Language (UML) is used to specify, visualize, construct and document an object-oriented software system. The design of the epSOS architecture benefits from this modelization and need also

§ *to develop a consistent meta-model,*

§ *to describe how the parts are expected to relate to one another (e.g. how does a business process relate to a service).*

Consequently, between various candidates, Archimate (<http://www.archimate.org>) was selected. Furthermore, because UML and Archimate adress different issues, this document refers to both.

⁴ Opengroup, *TOGAF Version 9*, 2009 (www.opengroup.org)

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

3.2 epSOS requirements derived from the Use Cases

This chapter reports the requirements derived from epSOS use cases, functional requirements outlined in D.3.1.2, D.3.2.2, D.3.4.2, D.3.5.2, D.3.6.2, D.3.7.2 and legal requirements stated in epSOS Concept Paper. The objective is to match specifications scope which has to be close to epSOS agreed use cases, but must not be too restrictive to enable beneficiaries to implement additional functionalities on a voluntary basis among their MS.


3.2.1 epSOS Use Cases

The present architecture document is based on epSOS Use Cases agreed within WP3.1 and WP3.2⁵:

- *EPrescription USE CASE 1*: medicine already prescribed in Country A. This use case describes the dispensing of medication(s) in country B when the medication(s) has been prescribed in a different country (country A), where the patient has a valid identification in terms of healthcare.
- *Patient summary USE CASE 1*: an occasional patient from country A has a medical episode in Country B; a single Patient Summary (the one of the patient's Member State affiliation) can be retrieved by the HCP of country B.

These two UCs are the ones that are specified exhaustively in D3.1.2. Nevertheless, operations used in this document can be assembled to fulfil remaining UCs.

⁵ Cf. Athens workshops minutes (01/01/09) from WP3.1 (ePrescription): "UC 1 will be the priority. UC 2 will be discussed, if left for Epsos expansion (...)" and from WP3.2 (Patient Summary) : "Only the PS of Country A (which is the MS of affiliation) will be shown to HCP of country B"


	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

For ePrescription USE CASE 1⁶, the operations below are assumed:

- HCP requests epSOS access authorization
- HCP requests patient identification
- The HCP checks the appropriate “confirmation of treatment relationship” checkbox on his/her software interface in order to validate the fact that the patient is aware that the HCP can now access his medical personal data.
- HCP retrieves a set of available ePrescriptions
- HCP chooses the ePrescription needed for dispense action,
- HCP retrieves ePrescription in his/her own language. Previously, operations below are assumed:
 - NCP-B checks HCP role and authentication
 - NCP-A checks patient identity, consent and right for HCP-B to access ⁷data according to its national (country B) policy constraints
 - NCP-A adapts ePrescription into pivot format
 - NCP-B checks Country A prescriber role against the Country B law to verify if it is a valid prescription also in Country B (ie. nurse as a prescriber)
 - On request of MS B a PDF document consent MUST be provided by MS A
 - NCP-B adapts pivot format into national form B
- HCP displays ePrescription for dispense action
- HCP gives medicine to patient (dispense action),
- HCP sends back eDispense through his/her Information System.
- NCP-B adapts eDispense to pivot format
- NCP-B sends eDispense to NCP-A

⁶ See D.3.1.2 Chapter 5 Description of the Use Case an requirements identification

⁷ Technically this corresponds to SAML assertion checking by NCPA processing message for medical data retrieve. This is consistent with operations described in D.3.6.2

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

For Patient summary USE CASE 1⁸, the operations below are assumed:

- HCP requests epSOS access authorization
- HCP requests patient identification
- The HCP checks the appropriate “confirmation of treatment relationship” check box on his/her software interface in order to validate the fact that the patient is aware that the HCP can now access his medical personal data
- HCP retrieves the Patient Summary along with the original copy⁹. Previously, operations below are assumed:
 - NCP-B checks HCP role and authentication
 - NCP-A checks patient identity, consent and right for HCP B to access data according to its national policy constraints
 - On request of MS B a PDF original document consent MUST be provided by MS A
 - NCP-A adapts patient summary into pivot format
 - NCP-B adapts pivot format into country B format

3.2.2 Use cases assumptions related to HCP identification, authentication and authorisation

Each Member State must ensure HCP authentication for trust establishment between countries. HCP identification, authentication and confirmation of access to the patient data are managed as local/national operations. Basically, these operations are the following:

- HCP is identified and authenticated through its local healthcare IT infrastructure

⁸ See D.3.2.2 Chapter 5.2 5.2 Agreement on the scope of the use cases and Chapter 5.3 Description of the Requirements and the Use cases

⁹ NCPs should support exchange of PDF documents compliant to PDF/A-1b. The PDF document MUST be provided by MS A on request of MS B.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

- NCP-B gets HCP attributes such as role to enable access to medical data. This operation is considered as authorization at national level (as described in D3.6.2).
- NCP-B is then responsible to send an assertion about the HCP identity/right to NCP-A

Referring to FR01 (*“the HCP must be unequivocally identified and authenticated in his local system and must be identified according to his role/profile”*) identification data for HCP must contain HCP role so that authorization for epSOS can be processed at NCP-B level.

Not only verification of identification of professionals must be done but also identification of health care organization must be taken into account¹⁰.

3.2.3 Use cases assumptions related to patient identification and authentication

The assumptions for patient identification at this step are:

- § The patient needs to be univocally identified in a reliable way (FR03: Patient Identification)
- § Country A is the only country where patients can be univocally identified¹¹. Therefore country A has to provide a way for HCP in B to identify the patient.
- § Identification information when available is to be given to the HCP, when this information is not available the HCP is not able to identify the patient through its IT

In terms of authentication, process is engaged in both countries (A & B):

- § In country B: patient identification is done by means presented by the patient to the HCP. A patient treatment relationship is established at the point of care by the HCP. This can be:

¹⁰ Cf. WP2.1 Sept 09 Concept Paper v.0.0.1/Annex A : National Contact Point : “NCP receives requests from and transmits replies to other NCPs in the form of verifications of Identification of professionals, patients and health care organisations (...)”

¹¹ Cf. D.3.1.2 Chapter 5.2.1.2. Description of use case: “Country A in this case is also the country where the patient can be univocally identified”



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

- either a human process by checking patient identity through identification document such as passport, national Id card, etc.
- or an authentication system by combining reflexive and cognitive factors such as digital certificates, pin codes...

NB: this first step is considered as “Authentication toward HCP” in D3.6.2

§ In country A: NCP A verifies patient identity and authentication attribute previously provided by country B. This is a national concern and it is processed according to country A policy.

Therefore in this document, the operations for a complete patient identification/authentication process below are assumed:


- HCP identifies and authenticates the patient
- HCP sends a sufficient information patient identification/authentication criteria needed by NCP-A to uniquely identify/authenticate the patient
- NCP-A sends confirmation or denial after check of transmitted patient’s identifier by national authorities or identity providers
- HCP is granted (i.e. authorized) or denied access to patient’s data.

3.2.4 **Use cases assumptions related to patient consent**

The cross-border access to a patient’s data requires additional authorization, based on patient consent¹². It is considered to be the legal basis for lawfully processing according to FR04 definition.

It is not the goal of epSOS to establish uniform Patient Consent practices for medical data. The mechanism for collecting patient consent is a national issue. Therefore, it is out of

¹² Cf. D.3.6.2 section 8.3 : Patient Consent

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

scope of the architecture to describe the whole process for patient consent but only the management of patient consent data is to be specified.

3 cases of consent are to be assumed¹³:

- a prior consent done in country A plus a consent given in B
- solely a full prior consent in A
- solely full consent in B

2 type of consents are admitted:


- 1) A sign XML assertion. This consent is created by the NCP B and A, on the fly and added with the transaction for the exchange;
- 2) A PDF document. This consent is the original document created when the prior consent was given by the patient. It persists under the country A side. The PDF document MUST be provided by MS A on request of MS B.¹⁴

EpSOS architecture specifications take into account the fact that cases of consents are to be managed within the system. What's relevant for specifications is that consent aims at being verified at NCP-A level consistently with national consent case, as a prerequisite of medical data disclosure for HCP. This operation participates to trust establishment (Cf. Concept Paper)

- § NCP-A checks patient consent according to its national policy (rules for health data disclosure). To minimize data processing, this checking, will be done before any semantic process (Cf. D3.6.2)
- § lifecycle of the consent must be logged in a way that the legitimacy of each request can be constructed in retrospect (Cf. FR04 Patient consent to access data)

¹³ Cf. Cf. WP2.1 Concept Paper Annex B : Patient Consent

¹⁴ Conclusion from TMP Taskforce Open Issues 100319

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

3.2.5 ***Supplementary specification related to trust between countries***

Trust between countries is defined as “*the agreed framework for creating trust by establishing policies for critical data protection, privacy and confidentiality issues as well as mechanisms for their audit*” (FR02 & NFR09 Trust between countries definition). Each MS is accountable to another MS and both must demonstrate that they meet certain agreed essential requirements.

Trust between countries concept gathers:

- HCP identification and authentication use cases assumptions (FR01)
- Patient identification and authentication use cases assumptions (FR03)
- Patient consent (FR04)
- Audit trail supplementary specification (NFR06)
- Security requirements and policies defined in WP3.7

Operations related to circle of trust are managed not only on national level (through national infrastructure) but also on NCP level:


- Role mapping
- Audit records
- Secured message within notably NCP signature

3.2.6 ***Supplementary specification related to data exchange/access***

PS and eP are to be exchanged in a structured form (FR05).

In the case of eP use case, Medication Summary (part of PS) does not have to be accessed separately by HCP (see FR11), except if two Member States agree to do it. EpSOS d3.x.2 does not provide specifications about Medication Summary for 2011 pilot.

For eP use case, the original ePrescription (FR12) is not send with the document but must be explicitly requested. Furthermore, the information about the dispensed medicine must

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

be sent to Country A (FR15). The original dispensed medication (FR17) is left to the responsibility of Member States.

Flows of communication are done between 2 NCPs and between NCPs and its national infrastructures. Therefore, the NCP must be able to locate and transmit data or messages.

If NCP-A is aware that not all available data can be provided, it will deliver as much as it can and it will inform NCP-B of the existence of further data by providing a status message with the response.

3.2.7 *Supplementary specification related to medical data transformation*

Three kinds of medical data are to be transformed (and consequently exchanged):

- Patient Summary – NB : Patient Summary can include Medication Summary
- ePrescription
- eDispense

When the NCP is acting as a provider of medical data it is responsible to correctly map national medical data into the epSOS pivot data structure maintaining clinical semantics.

When the NCP is acting as a consumer of medical data, it is responsible for having those data available in its country language and semantics. The national format for HCP is left to the MS decision (e.g: MS can choose to map epSOS pivot data structure into the national data structure and the nationally used coding systems).

3.2.8 *epSOS Core Business Blocks derived from FR/NFRs*

This section lists the requirements identified within WP3.1 and WP3.2 directly derived from use cases in order to have a complete view for the architecture document.



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture

Date: 30/04/2010

Functional Requirements		Fulfilment of the Requirement
FR01	HCP Identification and authentication	The epSOS Identification and Authentication profile enforces the HCP identification and authentication. A respective assertion MUST be provided either with each request or during establishment of a closed session.
FR02	Trust between countries	The epSOS Circle of Trust profile sets up a trust relationship among NCP operated gateways. Gateway-to-Gateway communication is through secure channels.
FR03	Patient identification and authentication	The patient is identified in country B according to the proposed mechanisms and processes of [epSOS D3.6]. The epSOS Patient Identification Handshake profile allows for the verification of additional demographics.
FR04	Patient consent	No access to medical data is granted unless a valid consent exists. epSOS Contract Confirmation Handshake allows to confirm a consent given in country A or to register a consent newly given in country B.
FR05	Structured information	The epSOS Medical Document Access profile provided transactions for the retrieval of structured documents.
FR06	Equivalent information	Out of the scope of this specification
FR07	Information understandable	Out of the scope of this specification
FR08	Information selection	The transactions of the Medical Document Access profile allow to return the documents in the query response
FR09	ePrescription presentation	Out of the scope of this specification
FR10	'Available' (and thus, valid) ePrescription	The epSOS Query Transaction can be used to query for any kind of documents that share any kind of common semantics.
FR11	Access to Medication Summary by dispenser	Medication summary is not considered as a mandatory application for the 2011 pilots. It is nevertheless assumed that some countries will pilot sharing of current prescriptions.
FR12	Original ePrescription	The Original Document option of the Medical Document Access profile and the Originator Authenticity profile define all the mechanisms to fulfil this requirement.
FR13	Identification of the	Out of the scope of this specification



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture

Date: 30/04/2010

	medicinal product	
FR14	Substitution	Out of the scope of this specification
FR15	Dispensed medicine data sent to Country A	The Notification transaction of the Medical Document Access profile allows sending information on the status change of an ePrescription to country A. The respective dispensation data MAY be send along with this notification.
FR16	Identification of ePrescription and medicinal product dispensed	The Notification transaction of the Medical Document Access profile allows sending information on the status change of an ePrescription to country A. The respective dispensation data MAY be send along with this notification.
FR17	Original dispensed medicine	Due to the continuous use of document OIDs and the inclusion of document relationship qualifiers with all documents the links between the different encodings and transformations of a document can be tracked.
FR19	Patient summary of country A available	Only the Patient Summary of country A is recognised and exchanged.
FR20	Information Traceability	All accesses to medical data are logged with audit trails.
FR21	Patient summary of country A available	The epSOS Medical Document Access profile allows querying a response with a patient summary document with a single business request.
Non Functional Requirements		Fulfilment of the Requirement
NFR01	Service availability	The epSOS stateless mode allows for continuing transactions even after a period of non-availability of certain services. The Warning and Information Option of the Medical Document Access profile allows proceeding in the case of partial failures.
NFR02	Communications	Communication is only through secure channels on layer 7. These channels are established between mutually authenticated gateways.
NFR03	Response time	The response time mainly depends on the details of the implementation of the epSOS services. Response time can be increased by using the epSOS statefull mode.
NFR04	Confidentiality	Medical data is encrypted during transmission between any two gateways.



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture

Date: 30/04/2010

NFR05	Access control	Any access to medical data is routed through a PEP that enforces all security and privacy policies that apply to the recent user session.
NFR06	Traceability/Audit Trail	All accesses to medical data are logged with audit trails.
NFR07	Integrity	All medical documents are digitally signed before transmission. NCP-A attests the authenticity and integrity of the original data.
NFR08	Non repudiation	Non-Repudiation is provided through audit logs and digital signatures.
NFR09	Trust between countries	See REQ FR02.
NFR10	Guaranteed delivery	EpSOS uses synchronous messaging only. Therefore transmission failures are detected. Each epSOS transaction follows an at-least-once semantics and can therefore be re-transmitted in case of a failure.
NFR11	Single session	NCP-A can detect multiple sessions for the same patient and reject the confirmation of more than one active treatment relationships at a time
NFR12	Supervision services	The epSOS Reporting Facilities extract data from audit trails that can be used to supervise the availability and performance of epSOS.
NFR13	Assistance services	Out of the scope of this specification


Initial reflexion toward architecture leads to the identification of the following three core business blocks¹⁵:

- Trust
- Data discovery and exchange
- Semantic / Data transformation

In addition, 2 more blocks are considered:

- Audit
- Support function

¹⁵ Cf. epSOS_Archi_Consolidated_Work_V04

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

The figure below illustrates how functional and non-functional requirements fit in core business blocks.

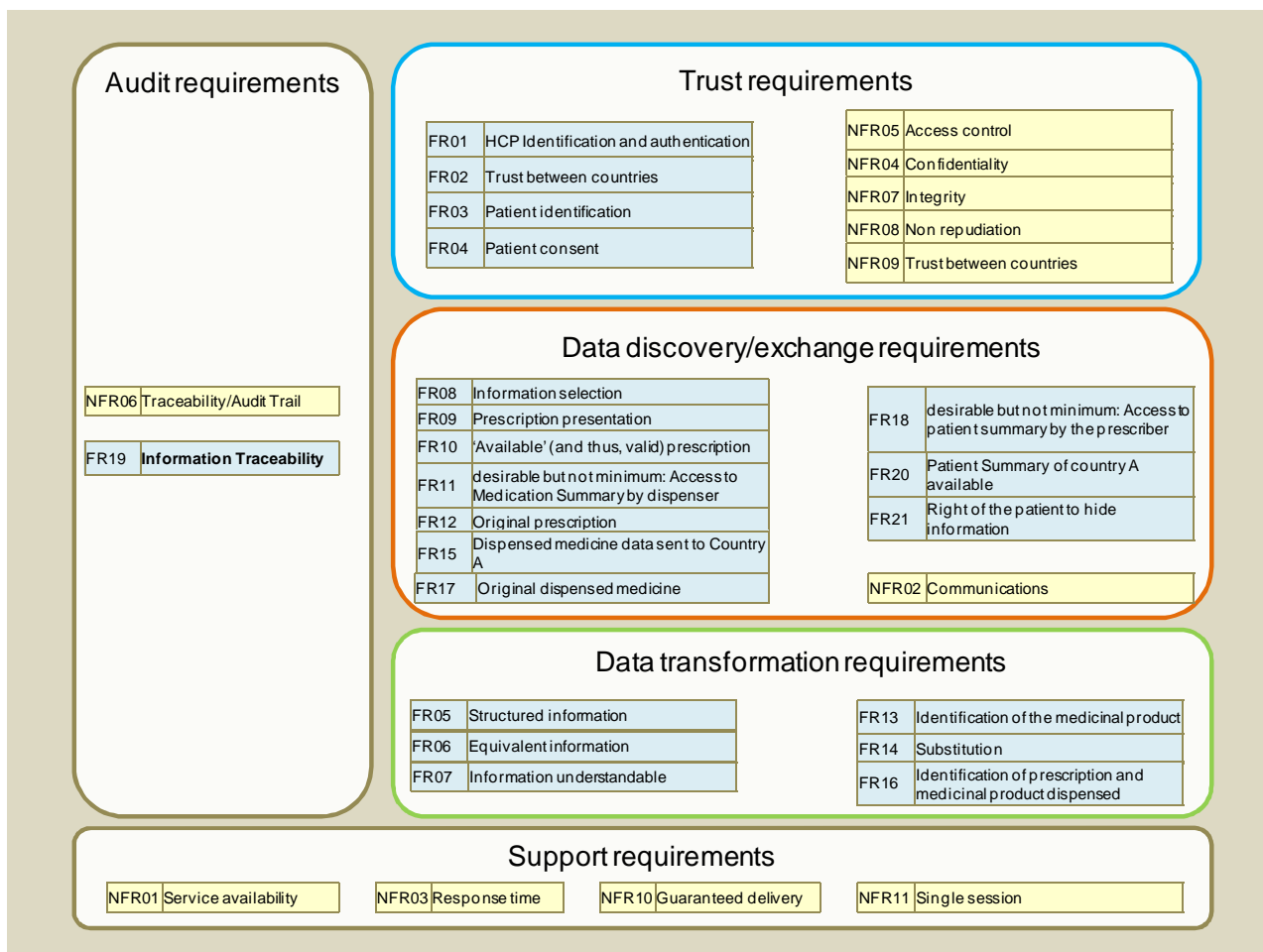


Figure 5: FR & NFR consolidated view

3.3 Basic Concepts and Principles

Regarding the aforementioned UC analysis and keeping in mind the establishment of a secure context, the following basic principles can be announced (from the general to the specific):

NB:

§ the following symbol **UU** states that the Requirement is considering mainly NCP to NCP communication.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

§ The following symbol : Ü states that the Requirement is considering mainly Internal MS information system to NCP communication.

Statement of Purpose

The epSOS system is based on 3 fundamentals principles:

- § epSOS will not require changes to national or regional legislation, although local rules of operation may be minimally modified,
- § epSOS will work as far as possible with existing infrastructure, only minimal additions or alteration will be required,
- § Information is exchanged but not shared. Any epSOS user (HCP(O)) MAY NOT modify an original document from abroad. The user retrieves a « read-only » document.

ÜÜ **REQ 3.3.1** Exchanges within epSOS are conducted between gateways (i.e. technical embodiment of a NCP) acting as technical operators that enable patient data to be accessed from whichever Point of Care of country B is participating in epSOS. Requesting gateways act on behalf of a HCP (at a PoC) who requires access to a patient’s medical data through epSOS. Responding gateways act as service brokers of an epSOS data provider.

: Ü **REQ 3.3.2** A National Contact Point (NCP) acts as a legal entity which creates a secure link between the epSOS trust domain from the national trust domain. It is the only component that has an identity in both domains. NCP of country A (NCP-A) acts as a data provider through its Inbound Gateway, providing the medical documents located in country A. NCP of country B (NCP-B) acts as a data consumer through its Outbound Gateway, used by HCP in country B to access medical documents provided by NCP-A.

ÜÜ **REQ 3.3.3** A single NCP MUST be provided by each MS within epSOS. The NCP acts as a gateway between the “epSOS side” (which exists in between 2



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

NCPs) and the “national side” (which exists only within MS). A trusted domain is set up between NCPs and its management is in scope of epSOS.

: **REQ 3.3.4** The national architecture outside the NCP is out of scope of this document (and epSOS in that matter).

REQ 3.3.5 Communications are processed between gateways and are synchronous.


REQ 3.3.6 Business transactions rely on a secure context (session) and do not handle security issues (only messages). All communications are encrypted.

: **REQ 3.3.7** On national side, a Member State MAY have multiple gateways outside the NCP - representing Member State’s health information systems, such as regional ones in order to identify and, later, access patient data.

: **REQ 3.3.8** Patient data belong to MS’s health information systems: each is identifiable univocally (it is a national responsibility) and implements gateways for in-out-bounds transactions (again, a national responsibility).

: **REQ 3.3.9** Patient data queries from a HCP in country B MUST go through NCP-B then NCP-A which, in turn, queries health information system from its own country. In other words, no query from HCP-B can be done directly to a MS’s health information system from country A. A trusted domain is set up between NCP-A and its national health information system. Appropriate level for management of trust and their influence remain under each MS responsibility.

: **REQ 3.3.10** Patient data (i.e. original, source data) are kept within their national existing infrastructure. HCP in country B may store the received and generated health data only to be kept for purposes defined by the current legislation in country B. It will be up to NCP-B to decide what information (if any) to store.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

Ü Ü REQ 3.3.11 A new eDispense document created in country B is attached to the notification transaction.

: **Ü REQ 3.3.12** Country A has the responsibility to update medical data of its own Health Information System with a new eDispense document.

: **Ü REQ 3.3.13** Patient Summary: for epSOS pilots, it is a NCP responsibility to release a single PS for retrieval. Only the PS of the patient country of affiliation will be taken into account. Each country sends back a single PS.

: **Ü REQ 3.3.14** Medication Summary is not supposed to be accessed by the HCP as a sole data object (as part of the Patient Summary). Transactions do not cover the retrieval operation to get only the medication summary.

: **Ü REQ 3.3.15** ePrescription: the reference use case is UC1 (ePrescription in country A, dispense in country B). EPrescription data are not modified by country B.

Ü Ü REQ 3.3.16 Transformation of the original medical documents to the epSOS pivot format **MUST** be done and signed under the responsibility of NCP-A. The original document (PDF documents compliant to PDF/A-1b¹⁶) **MUST** be sent with the transformed document (CDA format) for safety and security reasons. It is a national responsibility to do the mapping based on the pivot format, not an epSOS responsibility.

: **Ü REQ 3.3.17** HCP of country B either authenticates at NCP-B or NCP-B confirms a previously done authentication to a trusted Identity Provider in B.

¹⁶ Conclusion from TPM Taskforce open issues 100319



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

: **Ü/ÜÜ REQ 3.3.18** Patient identification process (see D3.6.2 section 9.10 for specific figure): Patient presents to HCP-B some accepted identification means (i.e. accepted by national policy of country A, such as eCard, passport, driver license or eID of future EU project such as STORK); if necessary a health specific ID may be given to HCP-B in accordance with the requirements of NCP-A. HCP enters the produced identification data into his/her epSOS interface (e.g. national web site, software connection); NCP-B queries NCP-A (“home country” for the patient) with entered data; NCP-A checks Patient ID and confirms to NCP-B which in turns informs HCP of country B. The ID query MAY come up with a new identifier (e.g. patient shows his/her driving license and ID query returns patient’s healthcare ID). In that case, this ID MAY be a temporal ID or pseudonym (issue to be considered by WP3.8ff).

: **Ü/ÜÜ REQ 3.3.19** epSOS MUST allow Patient Consent to be given in country A and/or country B (see D3.6.2 section 9.3). Patient Consent rules and procedures are determined by patient’s home Country A and may require consent given in country A prior to the episode of care or consent given at the point of care in country B. There is no need to transmit a consent document from country A to country B NCP-A MAY decide to reject the consent given in country B. A clear statement on the status of consent and HCP authorisation MUST be provided to the patient. Country A calculates patient consent timeframe validity. If previous consent in country A does not exist and the patient gives his/her consent status explicitly (in a digital format) in country B, then country B SHOULD inform country A of this new consent. EpSOS is supposed to deal with one consent per patient¹⁷, valid for all the documents. This consent represents a “Yes/No” value for country B.

¹⁷ Decision taken at the Paris Workshop (2009-12-15).



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

ÜÜ **REQ 3.3.20** NCP signatures are used to vouch for the authenticity of exchanged data. If a medical data is signed by the HCP, this signature **MUST** be verified. Regarding NCP signatures of the medical data it is assumed that:

- **REQ 3.3.20a:** *for the Query response*, no signature is needed (NCP-B already trust each other through NCP contract);
- **REQ 3.3.20b:** *for the Retrieve response*, NCP-A envelopes medical data and HCP(O) signature and adds its own signature; NCP-B **MAY** optionally sign the retrieve response document to be sent to the HCP. The original document ID **MUST** come with the transformed document Object ID for auditing purposes;
- **REQ 3.3.20c:** *for the Notification*, no need for signature;
- **REQ 3.3.20d:** *for the Dispense*, NCP-B envelopes medical data and HCP(O) signature and adds its own signature. NCP-A **MAY** optionally sign the dispense document to be sent to the HCP(O). Meta-Data are protected by message security.

ÜÜ **REQ 3.3.21** epSOS resources¹⁸ **MUST** exist for the cross-countries system to operate:

- a Routing Table in order to locate NCPs within epSOS,
- a list of the epSOS Trusted Certificates and a list of the revocation status of the certificates,
- a Taxonomy for the epSOS pivot format and the epSOS Master Value Set Catalogue and Master Translation Catalogue. Those services **MAY** be duplicated on the national side but **SHOULD** be maintained centrally,
- Information about the requirements of each country and acceptable forms of patient identification and consent,
- Support material for development and testing¹⁹.

¹⁸ To be defined within WP 3.8-3. JWG

¹⁹ Decision taken at the Paris Workshop (2009-12-15).




D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

: **REQ 3.3.22** Audit trail must exist for each transaction (such as trails related to identify information and trails related to business transactions like ePrescription or Patient Summary). HCP claims to be authorized by NCP-A which MUST write a specific audit trail that just keeps the mapping of processed Object ID (OID) onto a Patient ID. NCP-B writes authorization given to A and focuses on auditing for the purpose of protecting the HCP. Patient of country A view on country B's audit trail is out of scope. Accessing multiple audit trails is out of scope of epSOS.

: **REQ 3.3.23** Access without consent in the vital interests of the patient, where the patient cannot give consent follows the same process as the standard access to a PS (i.e. same HCP-B authentication sent to NCP-A), although the local consent confirmation is replaced by a consent override notification checked by HCP-B.

As a result, NCP-A rules MAY be more relaxed than the standard procedure for accessing a PS (e.g. less/no consent) in order to grant access.

REQ 3.3.24 The system must provide confirmation that a complete data set has been transmitted. An alert should signal any interruption or fault which may have resulted in some data being omitted.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

4. Business View

The Business View deals with how the business processes, associated individuals and business units relate to each other. The Business view represents the concepts that are supposed to be stable whatever the implementations or the Use Cases are applied.

The epSOS is designed to accomplish operational task driven by the business strategies. The business driven approach and the technology driven approach meet in order to logically and technically match business use case scenario.

4.1 epSOS Information Model

This chapter gives a high level representation of the epSOS information model, including domain actors (i.e. a person, a device, another system or sub-system) and objects.

4.1.1 *Actors, Roles and Objects*

Actors can act on the epSOS system or is acted on by the epSOS system.

A *role* is related to an actor having a specific behaviour in a particular context: provider and consumer. The epSOS system bridges the communication between formats based messaging under two modes of communication: Outbound and Inbound. The consumer (e.g. HCP(O) asking for a Patient Summary) uses the outbound actor (i.e. NCP-B) to query the inbound actor (i.e. NCP-A), then the inbound actor retrieves the medical data under its national infrastructure and acts as a provider. Simply put: the provider retrieves information from its own country and the consumer queries for information.

The definitions of involved actors can be found in the glossary (Chapter 8).

Actors are: Patient, HCP(O) (no distinction is made in this document with HCP/Institution), Infrastructures of country A and B, NCPs.

Objects are: Patient Summary, ePrescription, eDispense, Patient Consents (for PS, eP, eDispense).

4.1.2 **Relationships between actors & objects: Information Model**

As a consequence from the analysis of FR/NFR from D3.1.2 and D3.2.2, the architecture is able to consider the epSOS information model as described in figure 6.

NB: NCP-A and NCP-B are not represented here, but considered in relationship as follows:

§ NCP-A: Patient Summary, ePrescription, eDispense, Patient Identification, Patient Consent

§ NCP-B: HCP, HCPO, eDispense, HCP(O) authentication

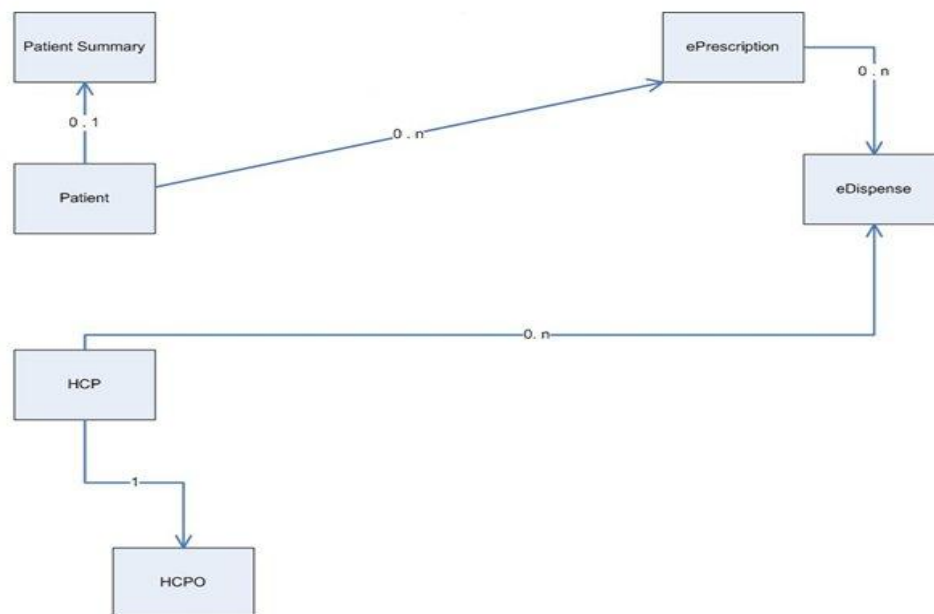



Figure 6: epSOS Information Model

NB:

§ Medication Summary is part of the Patient Summary but it is not represented as such in the above figure.

§ Patient consent (not represented here as a manipulated document – but used as attribute to an operation) contains the information about roles of the HCP.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

4.2 epSOS processes

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

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

- Secure context establishment
- Data Exchange and Handling

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

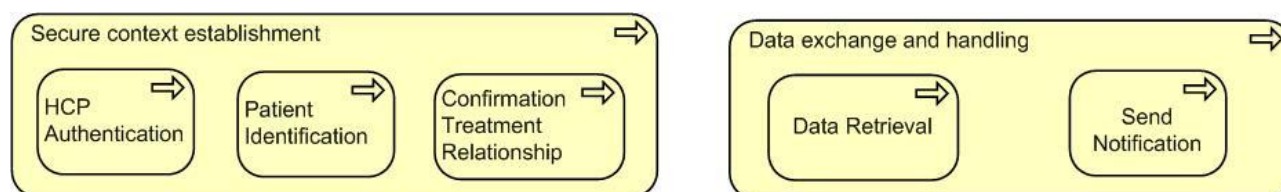


Figure 7: epSOS Core Business Processes

4.2.1 Establishment of a secure context between 2 NCPs

Within epSOS, the consumer (Query operations) and the provider (Retrieve operations) do not know each other. The Circle of Trust is among NCPs. They are solely able to establish mutual trust relationships. The final trust relationship is (n:n) and set up based on direct trust relationships among NCPs. The key issue is that an NCP can rely on the agreed behavior of another NCP.

While country B needs access control to protect its HCPs from accidentally accessing data in an illegal way (e. g. because the data controller in country A allows for an access that is forbidden by the law of country B), country A has to protect the privacy of its citizens and to ensure the integrity of its internally managed data objects.

D3.7.2 (section 6.2) details elements related to the trust secure context infrastructure and those security issues are treated in section 5.3.

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

REQ 3.3.25 The communication between 2 NCPs:

- MUST include mutual requestor/sender authentication (unique and non-repudiable identification) and MUST prevent attacks on the communication level,
- MUST include mechanisms for confidentiality, integrity and non-repudiation,
- MUST provide a unique identification and a non-repudiable authentication of HCP(O),
- MUST provide means to make a business request non-repudiable for the HCP,
- MUST ensure that the originator information of a medical data object is authentic,
- MUST ensure that a medical data object has not been modified while transmitted.

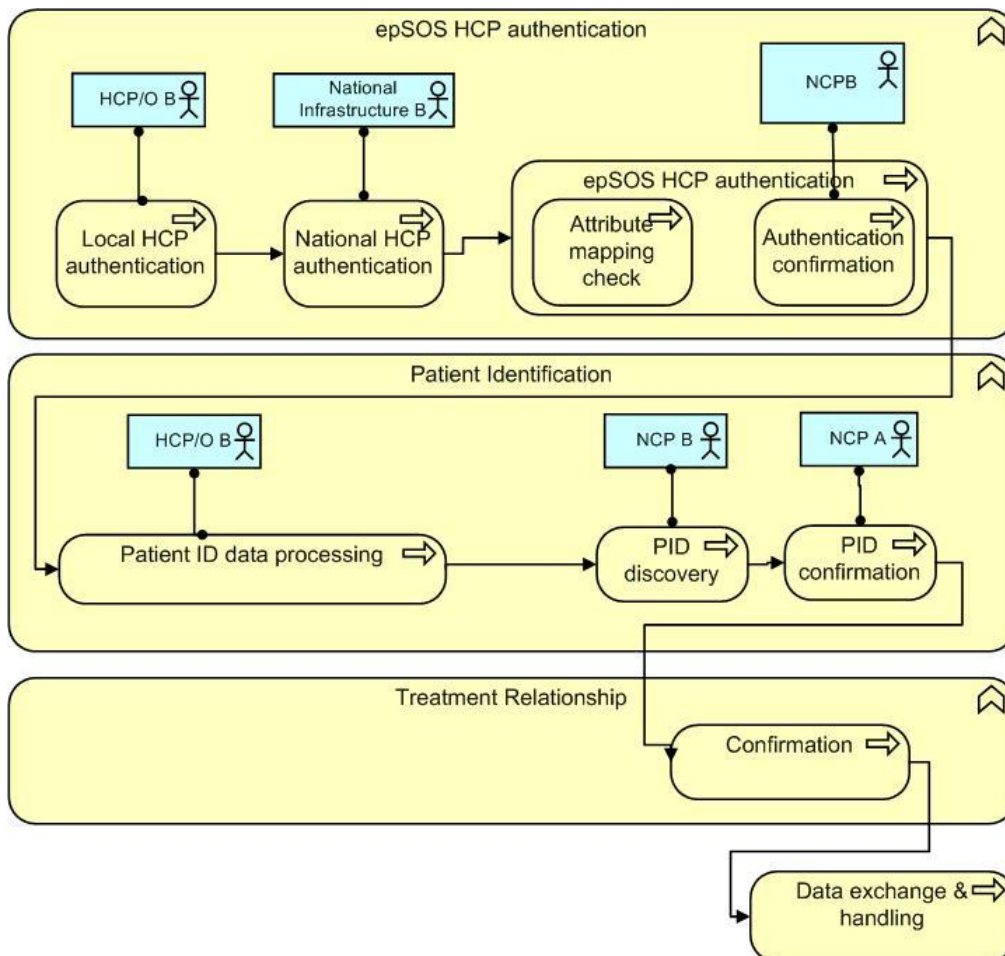



Figure 8: Secure Context Establishment

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

Basically:

- § Step 1: a HCP is identified and is authorized to access the epSOS System,
- § Step 2: A Patient Identification process follows,
- § Step 3: The Confirmation of the Treatment Relationship is established between the patient and the HCP(O)

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

The HCP authentication allows for the HCP(O) its authentication in country B. For the authentication of the HCP(O) - who issues the request - and for the authorisation of that HCP(O) by the patient - who is the owner of the requested medical data object - country A has to trust the processes of country B.

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

NB: A dedicated Patient ID transaction MAY be omitted in the following cases:

- § *identification by demographics and non-healthcare identifiers only*
- § *use of pseudonyms*
- § *multiple data sources (see document "WP3.3/3.4 Status and Requests for Discussion – Dealing with Multiple Data Sources")*

Omitting an explicit transaction on ID issues would limit solutions because epSOS would need to assume that the same patient is identified by different IDs in different countries - which requires an ID mapping.

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

required by country A) is done, initiated by the HCP(O) of country B but controlled by the NCP-A.

The Treatment Relationship Confirmation is established between the HCP(O) and the patient. A treatment relationship is validated when the HCP(O) checks the box provided by his regular interface.

4.2.2 Medical data exchange & handling

Medical data exchange & handling is the core business activity of epSOS. This does include PS and eP exchange. Two groups of processes have emerged to handle data exchange.

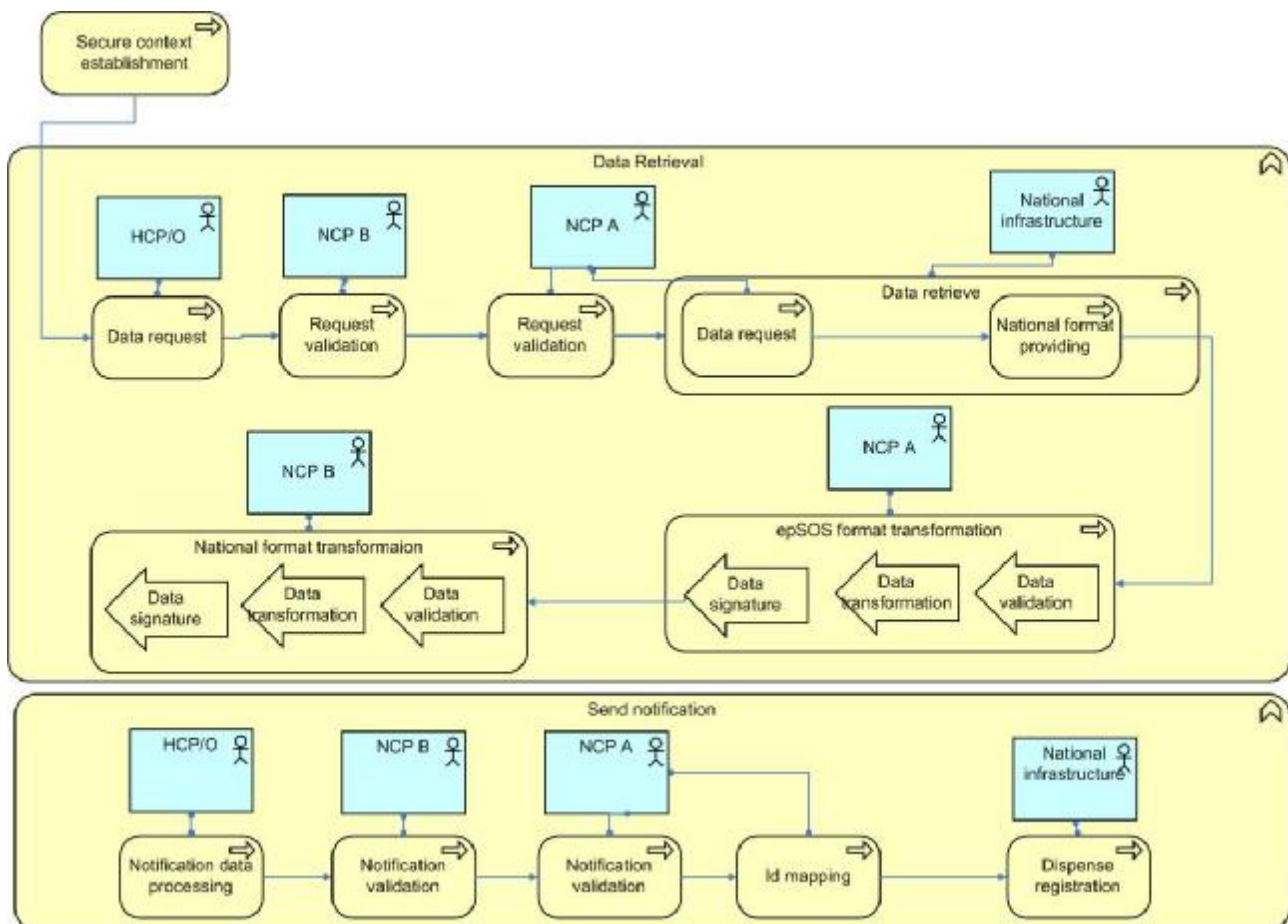



Figure 9: Data Exchange and Handling

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

Data retrieval


HCP(O)-B gathers information liable to be treated by NCP-B. Local infrastructures have many different ways to process their medical data. NCP-A must be able to treat data even if data source or format changes. First an automated task, called Discovery, is operated on retrieved local/national format. If no exception arises, then the data transformation to the epSOS format can start.

Data transformation has a set of rules for transforming a national format into an epSOS format. The transformation is achieved by associating national patterns with templates (validation). The structure of the epSOS pivot format (CDA envelope) can be different from the structure of the national source document. Elements from the PS & eP can be filtered; reordered and arbitrary structure can be appended to fill up the epSOS format. A signature for the document is then provided at the end of the process. Data is always displayed synchronously, and MUST adapt various technologies.

NB: The processes described in this section have a general value for epSOS. However, Privacy Law of some MS MAY require that data transformation is performed not in the NCP, but in the system where the information is kept or in the system where the information is exploited.

Send Notification

The notification supports the ability to notify – typically Country B – a change of status on the data retrieved from Country A (i.e. an indicator referring to a state transition). It also supports the ability to send data originated in Country B to Country A (e.g. dispensation/supply).

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

4.2.3 Groups of epSOS processes

As a summary, the identified building blocks can be sorted out as in the following figure:

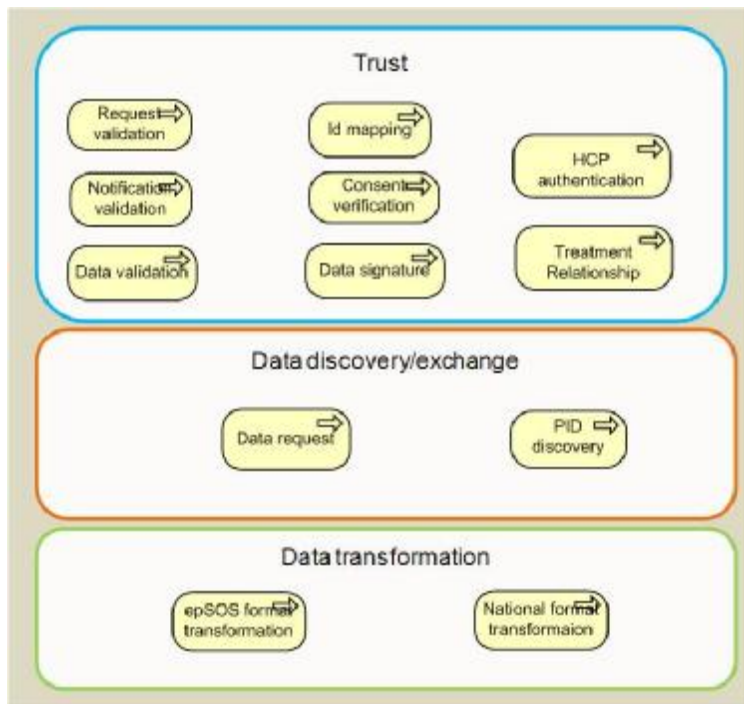


Figure 10: Processes supporting core building blocks

4.2.4 Description of the flow of control

The following figures provide a view of data processing and secure context through the data exchange request.

HCP Identification & Authentication

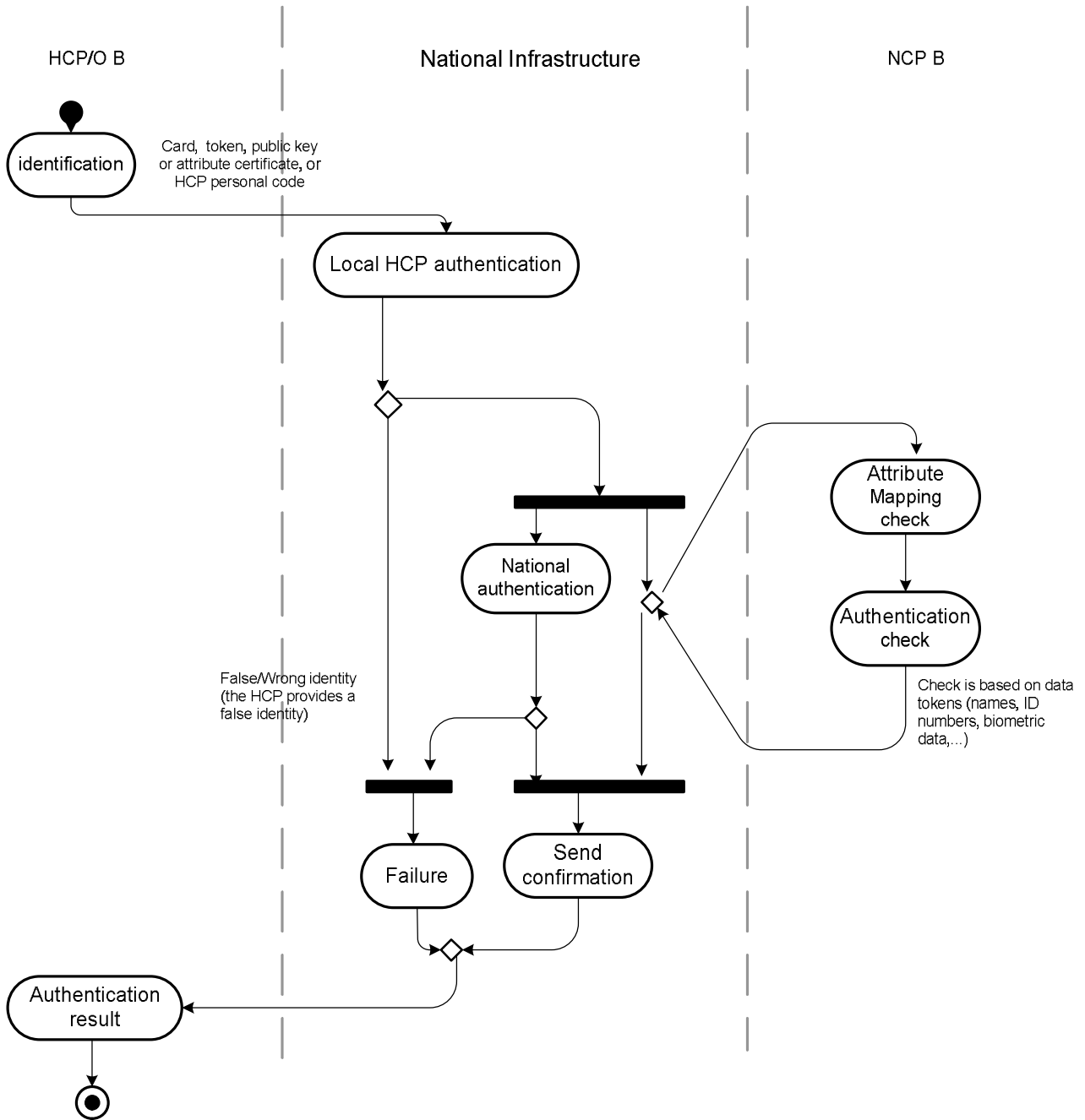


Figure 11: epSOS HCP Identification & Authentication

At the beginning of the process, identification procedure initiated by the HCP is insufficient to face the threat of a false HCP identity. The authentication can solve this problem. HCP



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

provides identification information and NCP verifies the formal correctness of provided information through the attribute mapping check operation. The proclaimed identity and genuine identity of the HCP will be validated during the authentication check step of the initial protocol. The identification/authentication result will be finally sent back to the HCP(O) B.

NB : HCP(O) and Infrastructure A/B parts are MS concern. The processes involved are presented as guidelines with no mandatory requirement.

Patient Identification

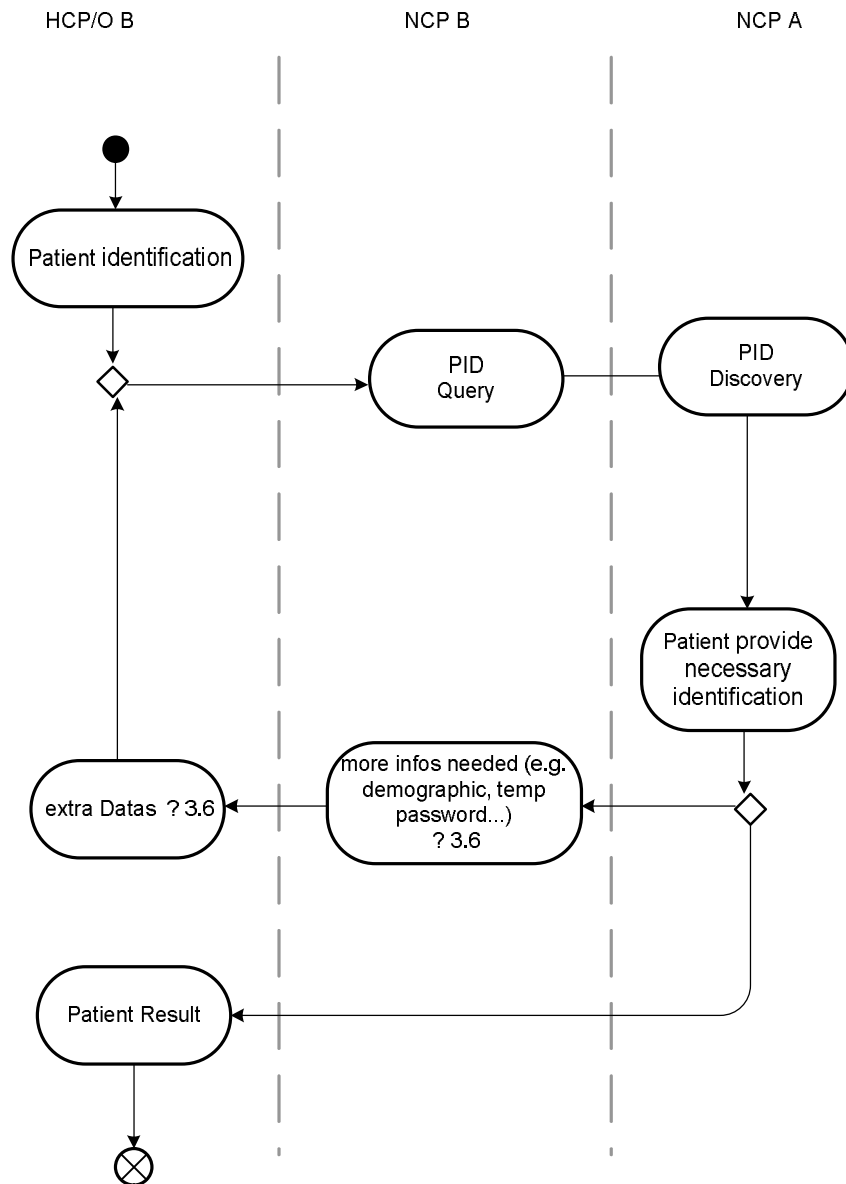


Figure 12: Patient identification

When a patient needs a health service (health care, ePrescription) in a foreign country B two sub-cases are considered:

- The HCP receives necessary identification information and is able to identify the patient.
- Patient identification information is not enough according to country A regulations and requires additional data (e.g. temporary password). MS can use TAN



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

(Temporary Access Number) for patient authentication. It is not a mandatory field and MS are free to choose traits for their citizens.

Only Identification of a patient by a HCP in country B is represented in this schema.

NB : HCP(O) and Infrastructure A/B parts are MS concern. The processes involving them are presented as guidelines with no mandatory requirement.

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

Treatment Relationship Confirmation

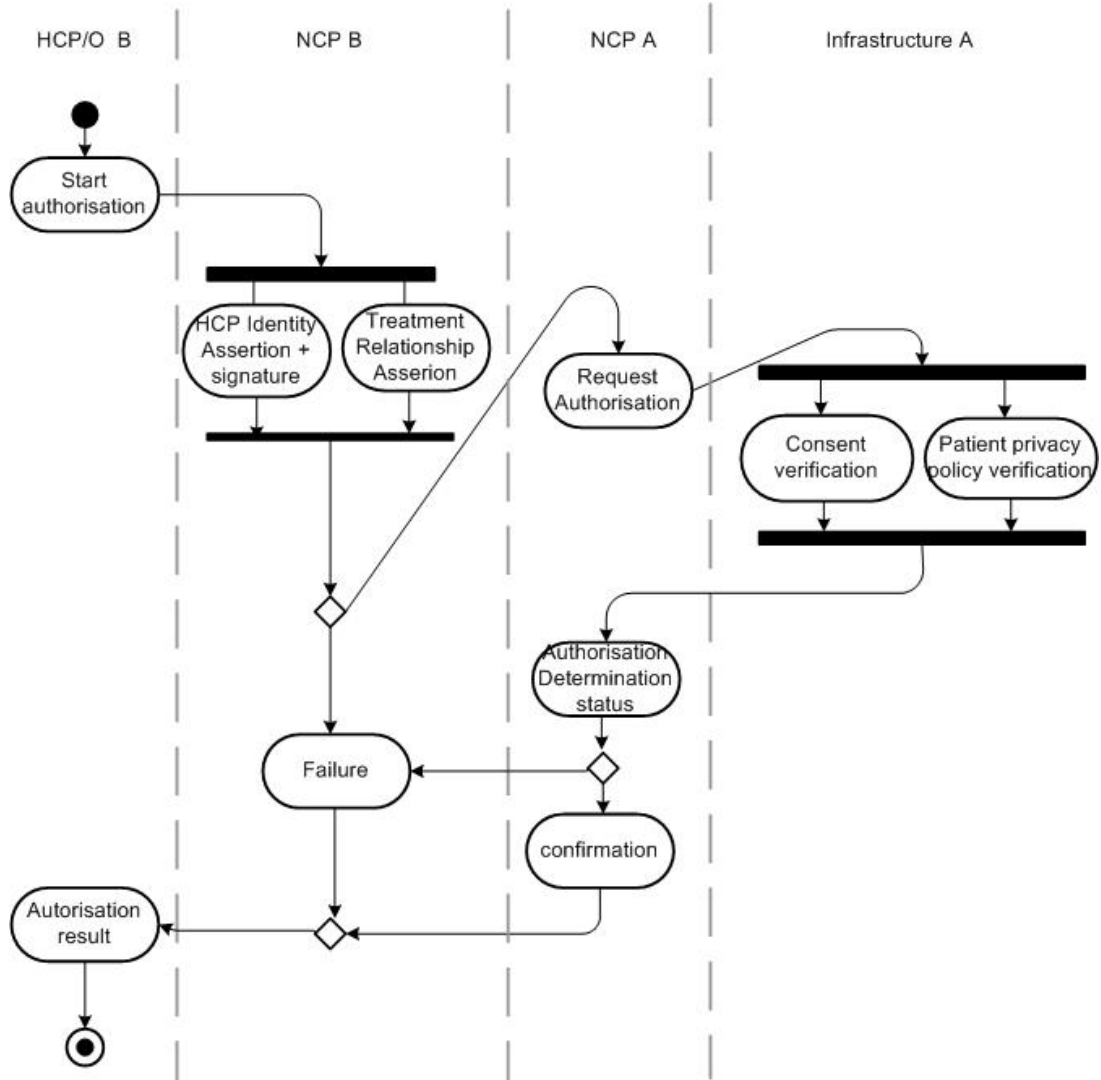


Figure 13: Treatment Relationship Confirmation

A treatment relationship confirmation issue by HCP(O) informs the patient that his medical data will be accessed. The patient MUST be informed to give his consent for this operation. The identity of HCP(O) with a signature is also encapsulated in the message. The signature of NCP-B MUST be recognized by NCP-A. When the message reaches country A, the Patient privacy policies state who can benefit the right to access his/her data's. A patient has to state his consent for the exchange of his/her medical data in accordance with the patient consent policy in country A. According to the type of data that needs to be accessed, country A determines the status as a result of consent and policy



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010
WP3.3: System architecture		

verification in country A. In addition to the Actors role, confirmation or rejection depends on the type of data.

The confirmation assertion as defined in D3.4.1 will be part of D3.4.2 (some extensions may be intro-introduced). It will be mandatory for country B to provide this assertion, but country A MAY decide to ignore it. An attribute that will be used for indicating an emergency access scenario (already defined by D3.4.1) will be included in the TRC assertion.

NB : HCP(O) and Infrastructure A/B parts are MS concern. The processes involved are presented as guidelines, MS states if they deliver Medical Data for the patient.

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

Data Retrieval

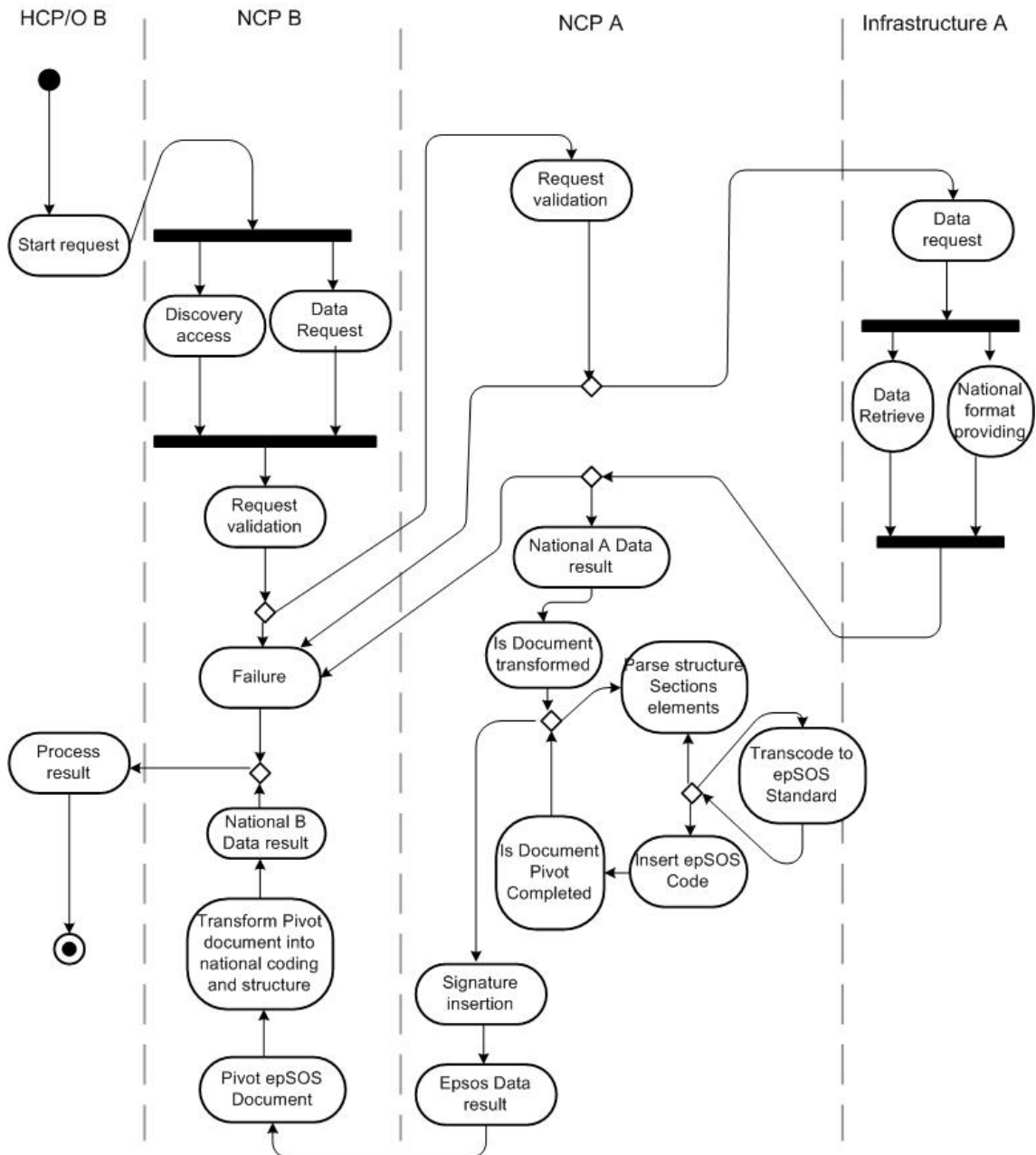


Figure 14: Data retrieval

The data retrieval process returns medical data under National Format.

The steps to follow in order to achieve the semantic transformation process are provided here:



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

- 1) The medical document is retrieved by NCP-A. The document MAY be digitally signed.
- 2) The nominal process is the following: NCP-A verifies the validity of the signature and checks the authenticity and integrity of the document. In case of a successful verification NCP-A signs the document.
- 3) The document is transformed into the epSOS pivot format by NCP-A (format defined in D3.5.2, CDA)
- 4) The original document is provided as a PDF or rendered as PDF and enveloped.
- 5) NCP-A creates a detached signature over the pivot document, the PDF document and the original signature. If PDF is provided by the system, there is no need for NCP-A to sign it. This attests that: authenticity and integrity were checked and the pivot document is a transformation of the original document.
- 6) Both documents (original and pivot) and signatures are sent to NCP-B.
- 7) NCP-B transforms the pivot document into country B native format and handles it over to the HCP.

Transformation and data validation are specific to each country (various national formats in use). The retrieval task is a national concern and in any case Country A is responsible to provide the result or the exception/failure outcome back to the requestor (Country B).

As proposed by WP3.5, the sequence diagrams for the transformation / transcoding operations at NCP-A and NCP-B are described in the two figures below (source WP3.5):

NOTE : To avoid multiple dispensation for the same prescription, pharmacist retrieves ePs and dispenses. A policy will be defined that a pharmacist always MUST first retrieve the current list of available prescriptions before he can dispense anything. This is in line with the Industry Team proposition that it is up to the pharmacist to manage its stock and that state machine and eP lifecycle management is to be done in Country A. D3.1.2 will be revised accordingly (no E2E-sessions, HCP-B policy).

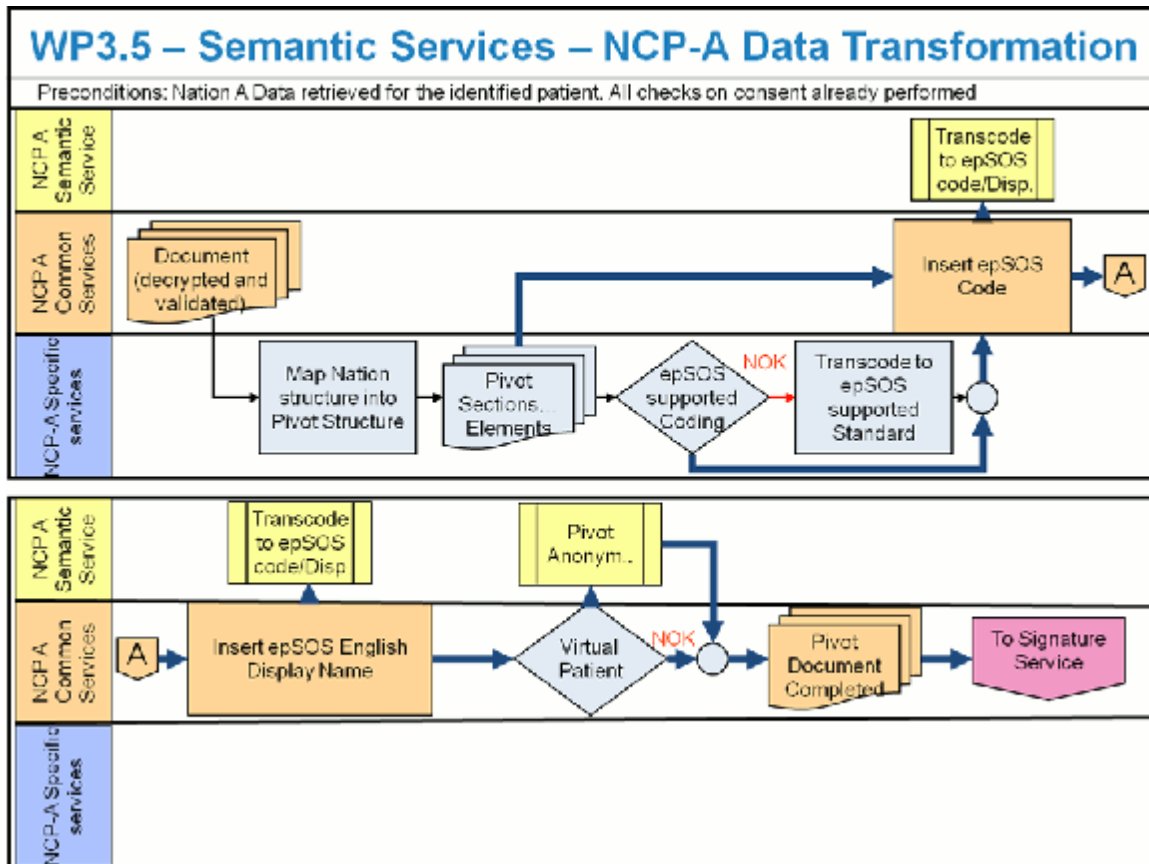


Figure 15: Semantic Services – NCP-A Data Transformation

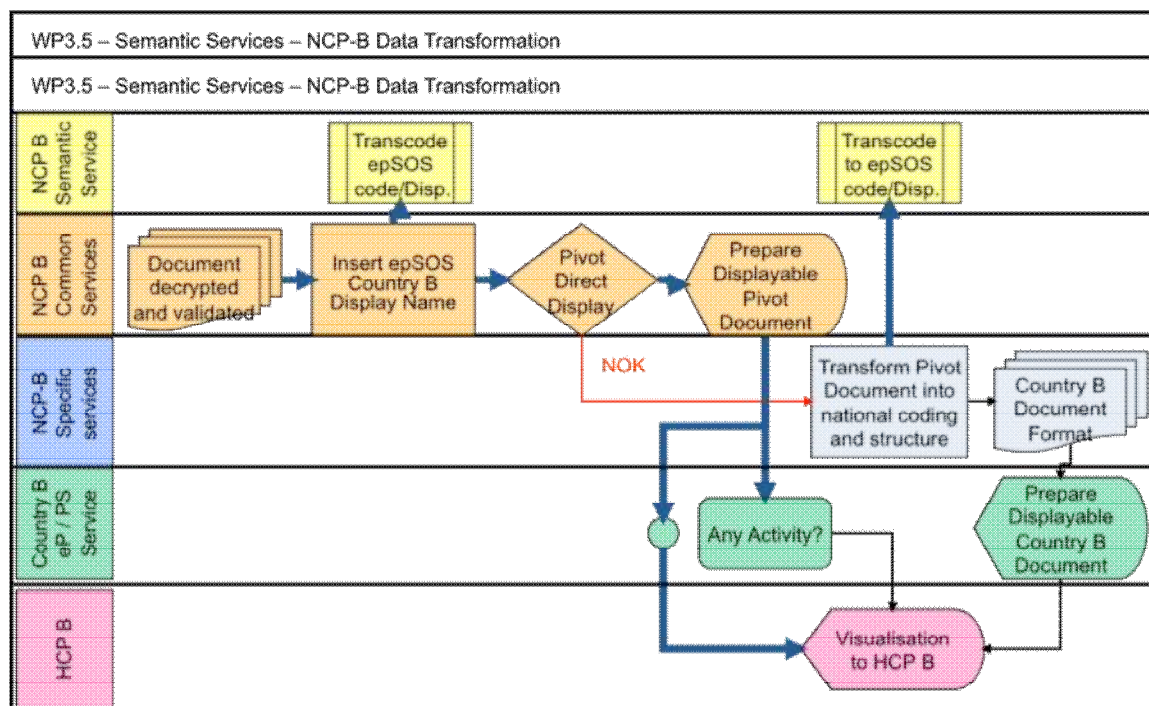


Figure 16: Semantic Services – NCP-B Data Transformation

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

NB: HCP(O) and Infrastructure A/B parts are MS concern. The processes involving them are presented as guidelines with no mandatory requirement.

Send Notification

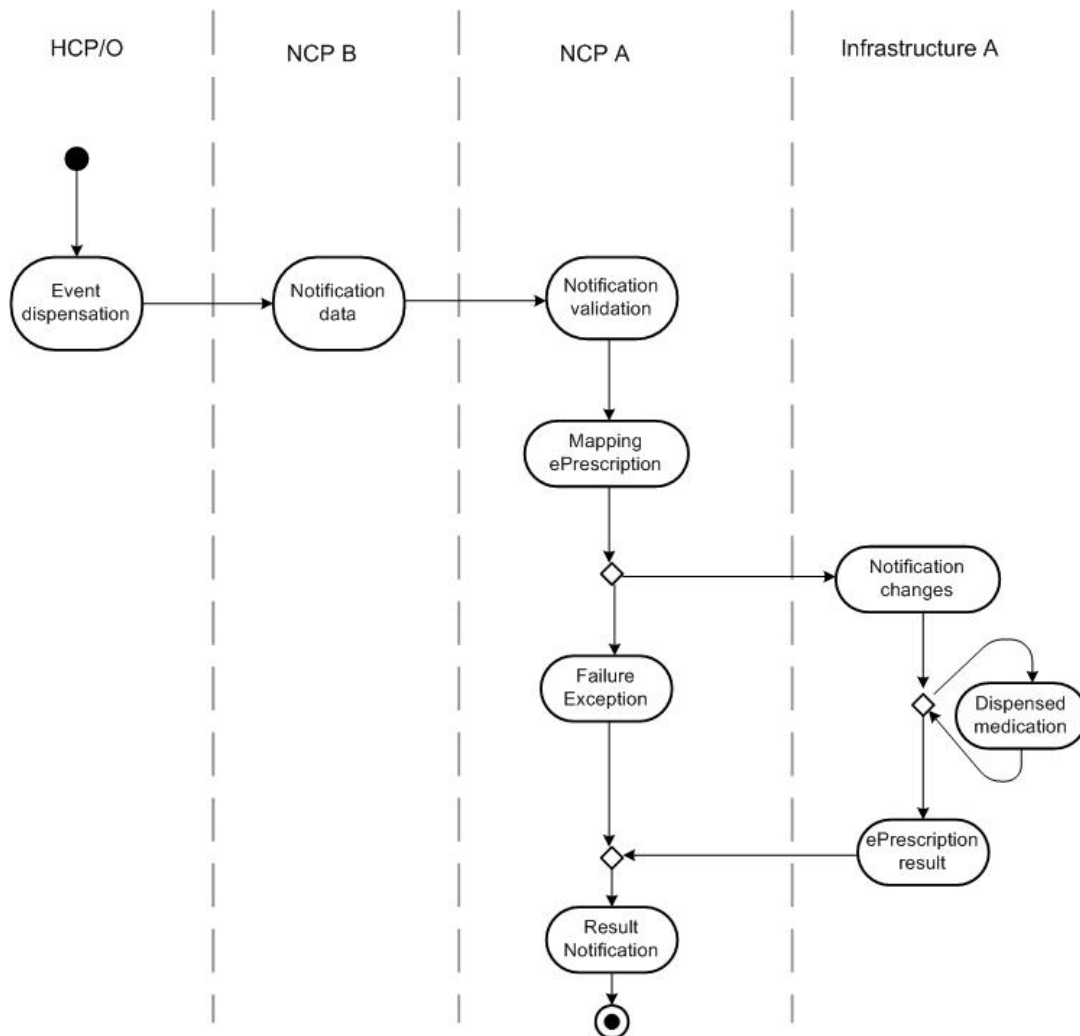



Figure 17: Send Notification

Notification occurs when an event is triggered (e.g. a dispensed medicine in country B). The notification object is then transported from B to A and verified. Because partial dispensation of a medicine is possible, Country A must provide a way to update the ePrescription.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

Unless the Notification result has been sent, no more dispense for the same ePrescription will succeed the validation process in country A.

NCP-A gives its ok ("Notification validation"); NCP-B does not wait for eP result (no return arrow from A); NCP-A assures updates ("Mapping ePrescription").

NB : HCP(O) and Infrastructure A/B parts are MS concern. The description of functionalities is presented as guidelines but presents no mandatory requirement.

4.2.5 **Exception Handling**

EpSOS has to be secure even if a failure arises. That is, the involved actors should stay in a well-defined state with a well-defined fault handling. Therefore exceptional events **MUST** be reported among system components in a way that allows the systems that are affected by the failure to process the respective message in a way that:

- § an appropriate reaction can be taken,
- § further dependent failures are prevented,

as few system components are affected as possible.

To reach this objective, 5 general principles for epSOS exception handling have been defined:

REQ 3.3.26 There are NCP-related exceptions, which **MUST** be defined in this epSOS-document. There are National-Structure-related exceptions, which **SHOULD** be covered by the national infrastructures. For each exceptional solution (i.e. long response time), the epSOS exception handling specification **MUST** provide guidance stating i) if it **MUST** be communicated among gateways or ii) if it **MUST**, **SHOULD** or **MAY** be handled solely within the affected national infrastructure.

REQ 3.3.27 epSOS services system **MUST** provide all system user and system partners (i.e. HCP, NCP and National Infrastructures) with appropriate feedback, even if the transaction failed.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010


REQ 3.3.28 An error feedback system must be established, including the support of a national helpdesk. A hierarchy of error messages (3 classes) should be established which is easily understandable to the HCP user, making clear when the user should abort the system:

- § Class I: *Try-again*, if it is a temporary error-producing situation (e.g. service not available),
- § Class II: *user-centric advice*, what went wrong (e.g. failed identification),
- § Class III: *call to higher instance* as something fundamental went wrong (e.g. national hotline). It is not mandatory for each member state to support such a “hotline”, but it is mandatory to specify a national contact if a fatal error must be propagated.

REQ 3.3.29 The decision to propagate an error-message is related to its code severity. There are five levels of severity in epSOS defined (cf. table below). It is mandatory to propagate the last “CRITICAL” Level. Every bilateral agreement between two member states can define to give one of the severity levels a dedicated action.

Severity Code	Description
Debug	Only for internal use (technical experts)
Info	Only for internal use
Warning	Some flaws, but the transaction is performed
Error	The transaction may or not succeed
CRITICAL	Critical failure, transaction must be cancelled

REQ 3.3.30 Trust between member states is essential for epSOS, especially in a failure situation. Therefore every failure **MUST** be recognized in the Audit Trail. It might be sufficient to just use a general error code with participants, date and time. But regarding to the severity code, it can also be most important to log as much information as possible.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

4.3 Synthesis: Business view

A classical distinction is made between “services” considered at the business level and those considered at technical level (i.e. Information System view and Technology view). Referring to OASIS-SOA-RM, “*Services are the mechanism by which needs and capabilities are brought together*”. The services enable distributed capabilities that may be under the control of different ownership domains. Service provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.

The main services for epSOS at a business level are represented in the figure below:

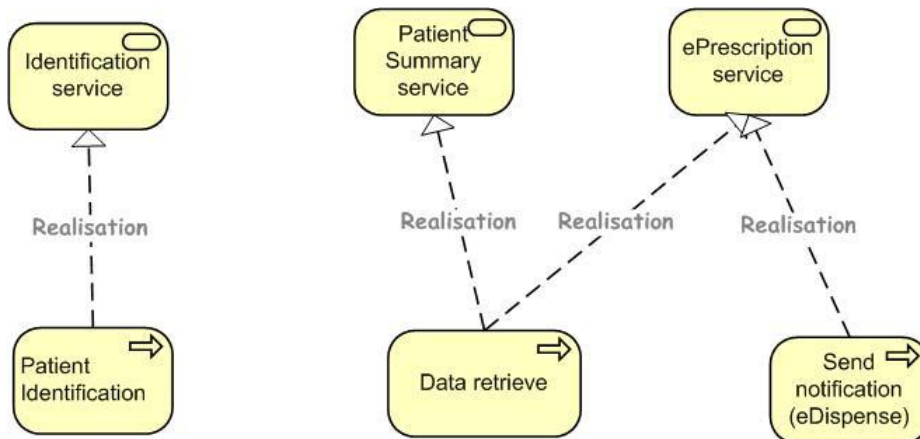


Figure 18: The epSOS services at business level

- **Identification Service:** This service first enables NCPs identification/authorization/authentication from HCP(O) of country B to National Infrastructure of country A. To enable exchange of data, the binding service creates a channel of communication, as a secure way to enable the circle of trust.
- **PS Service & ePrescription service:** data are sent through the PS & ePrescription services. Those services check for the validity and the transformation to the pivot format back and forth.

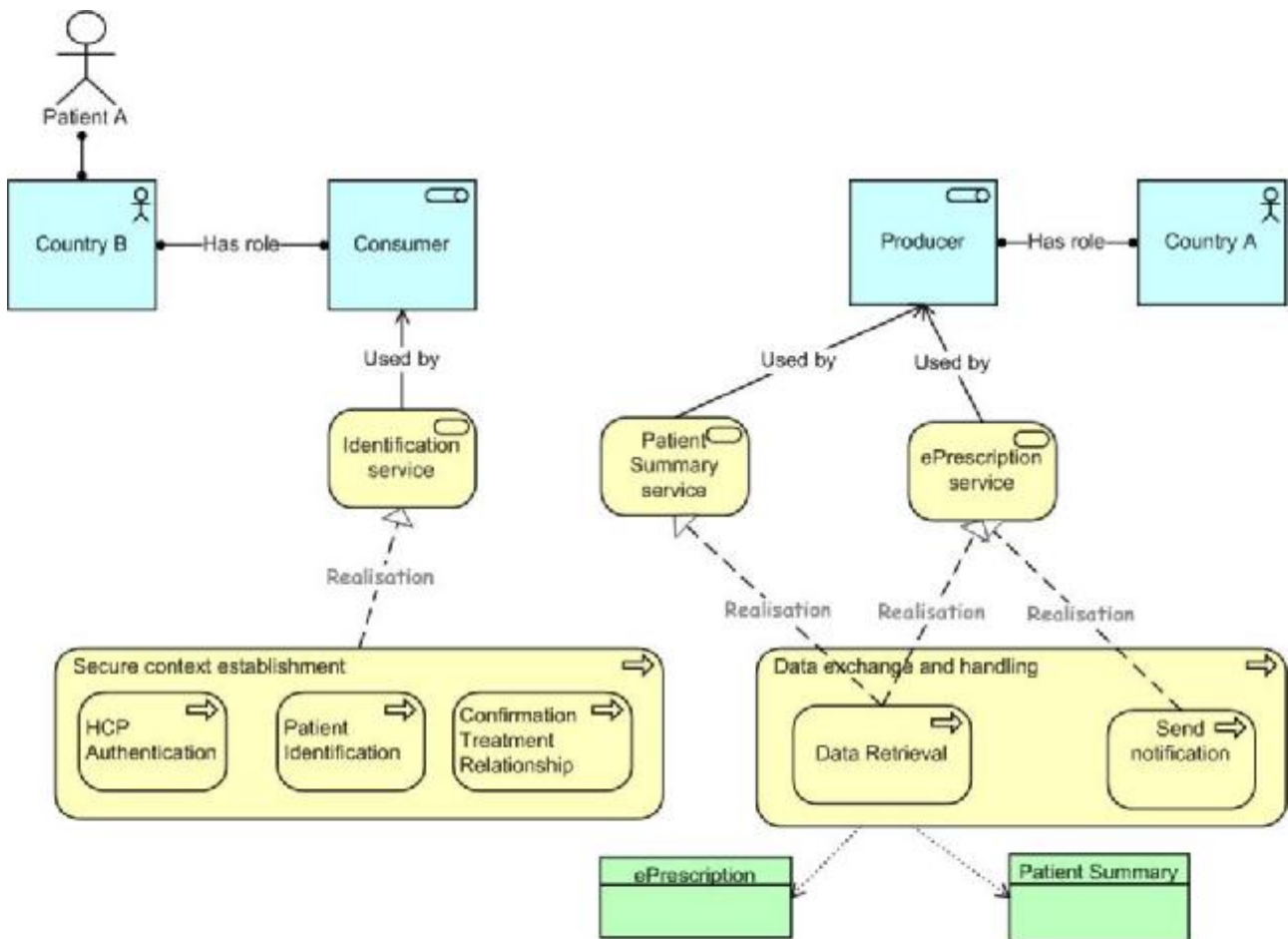



Figure 19: epSOS Business View

As stated before (see above, Secure Context Establishment figure), it has been chosen not to have the Circle of Trust security service appear in order to help reading the overall epSOS business processes.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

5. Information System View

The Information System View provides a blueprint for the individual application systems to be deployed, the interactions between the application systems, and their relationships to the core business processes of the organization with the frameworks for services to be exposed as business functions for integration. Because of the sensitive context of transmitting medical data special attention is given to security and legal issues (e.g. levels of trust, operator access rights, and patient consent). The cross-country exchange of medical data does not only provide legal challenges but first and foremost problems regarding the structure and content of such information. WP3.5 Deliverables describe the pivot format for the information exchange.

This chapter defines the structure and the high level behaviour of an NCP while the next chapter (Technology View) defines the technology mapping.

5.1 From Business view to epSOS Information System view

The business view focuses on the groundwork, according to the considerations from WP 3.1, WP 3.2 and 2.1, from which the basic blocks of application services are identified. Each block described in the Business View requires *Services* to operate.

A *service* represents a unit of essential functionality exposed to others participants from which the epSOS Architecture is structured.

The highest level for epSOS services is consistent with the building blocks introduced previously. The information system view of epSOS focuses on NCP services. The blocks are the basis for NCP services structure therefore applicative functions described in this chapter are related to one of the following parts of an NCP:

- epSOS NCP interfaces
- internal NCP service architecture
- National interface

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

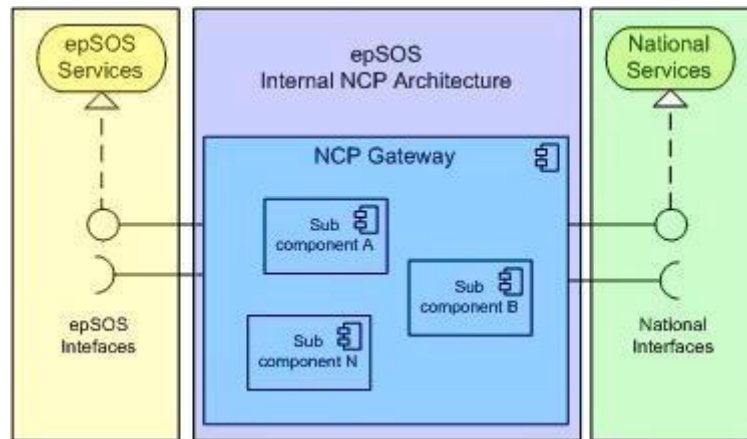


Figure 20: epSOS NCP basic structure

The *epSOS NCP interfaces* regard to services provided and consumed by other NCPs of the epSOS infrastructure. epSOS interfaces are “normative” for an epSOS NCP. An NCP is a “participant” of epSOS world *if and only if* it is compliant to normative epSOS interfaces in terms of structure, behaviour and security policy. The main part of this service is related to NCP to NCP exchange, but some common utility services can be centralized now or in the future²⁰.


The *National interfaces* are the services provided and consumed by an NCP in the “National world”. The implementation of these interfaces, obviously, strictly depends on the specific characteristic and standard adopted by every National Infrastructure.

The internal NCP service architecture defines a structure of sub components and relative internal interfaces of an NCP. This set of specification supports the realization of Common Components and can be viewed as a facility for epSOS.

Obviously an exception is the subcomponents for the realization of National Interfaces realized on a National basis.

The responsibility of this part is to implement:

²⁰ See next section.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

- the business logic (data discovery / Exchange / Transformation services) necessary to expose and consume the epSOS NCP interface with the necessary protocol, schema and terminology mapping from and to the National protocol, schema and terminology .
- trust services (security) for the handling of the defined security policy (epSOS and National)
- audit Services for the realization of the audit requirement
- support (utilities) internal services

The figure below is a high level representation for epSOS communication across NCPs, Country A and Country B with a more detailed view of the NCP services structure.

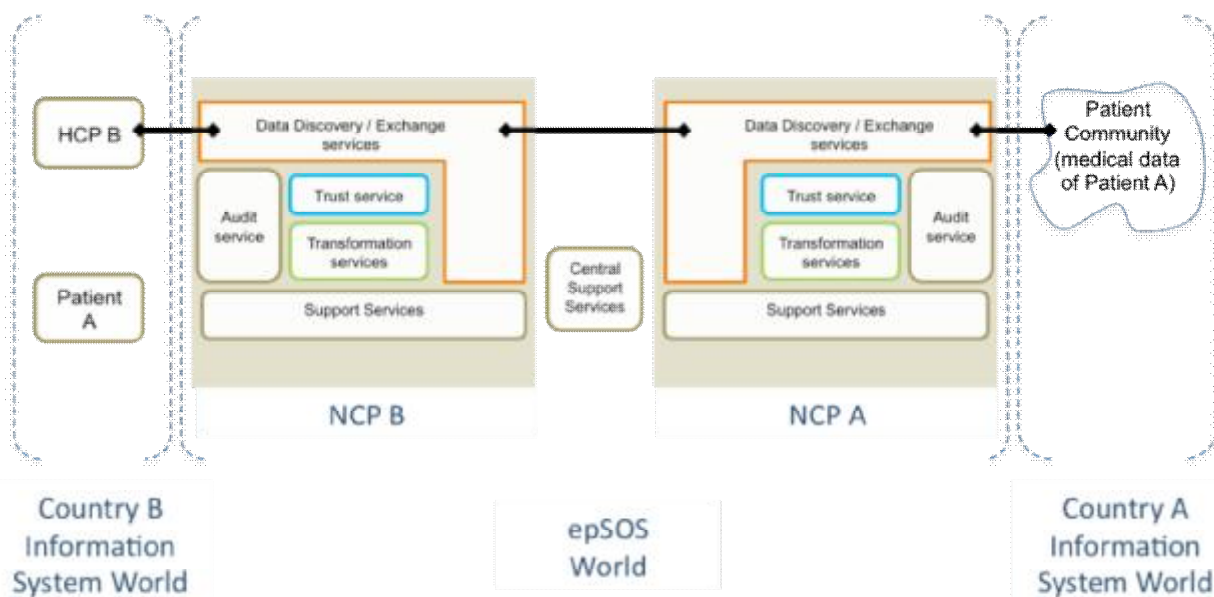


Figure 21: epSOS logical view

- § Data discovery / exchange: group of services to enable message sending either within the country or outside, to another NCP. It includes Patient Identification service.
- § Trust services: ensure trust and notably message or data validation, verification, signature, mapping

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

- § Transformation: gather the services for data object schema providing (epSOS pivot format or national format) and taxonomy mapping
- § Audit: bring together all the application services needed for system traceability
- § Support: gather the application services needed to ensure service availability, response time, guaranteed delivery and session to access epSOS

Each NCP in epSOS World can play the role of consumer and provider of epSOS services and, in the same way, impersonate the corresponding role of consumer and provider of National services.

As a consequence, NCP services are parted in internal services and external ones.

The figure below illustrates the separation of concerns between epSOS world and national World. It is not the scope of this section to be yet specific about internal and external services. Figure 24 will serve that point later in the document.

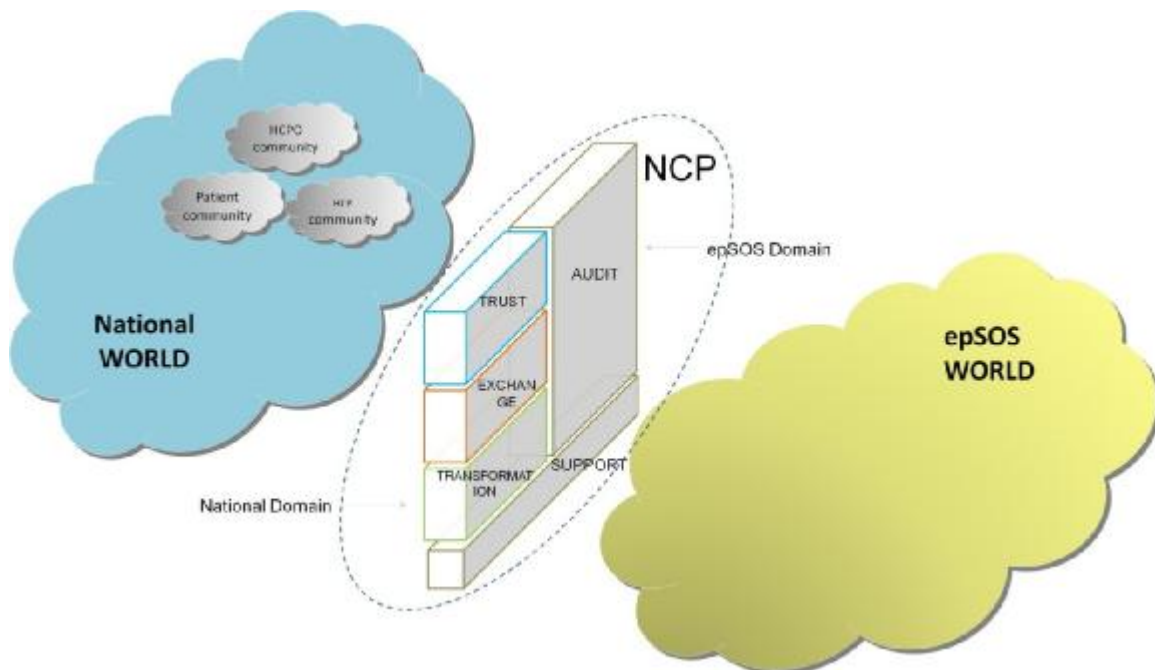



Figure 22: Services regarding national and epSOS domains

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

5.2 Descriptions of the epSOS services

In the following sections the elaborated epSOS services are subdivided into Trust & Audit (covering services related to security issues) and Data Exchange & Transformation (covering services related to any data exchange out of or through the epSOS domain). Furthermore the services are subdivided into internal (living within the epSOS domain) and external (living within the national domain) services. Some services are related to both domains.

Support services are discussed in the section dedicated to epSOS Central Services.

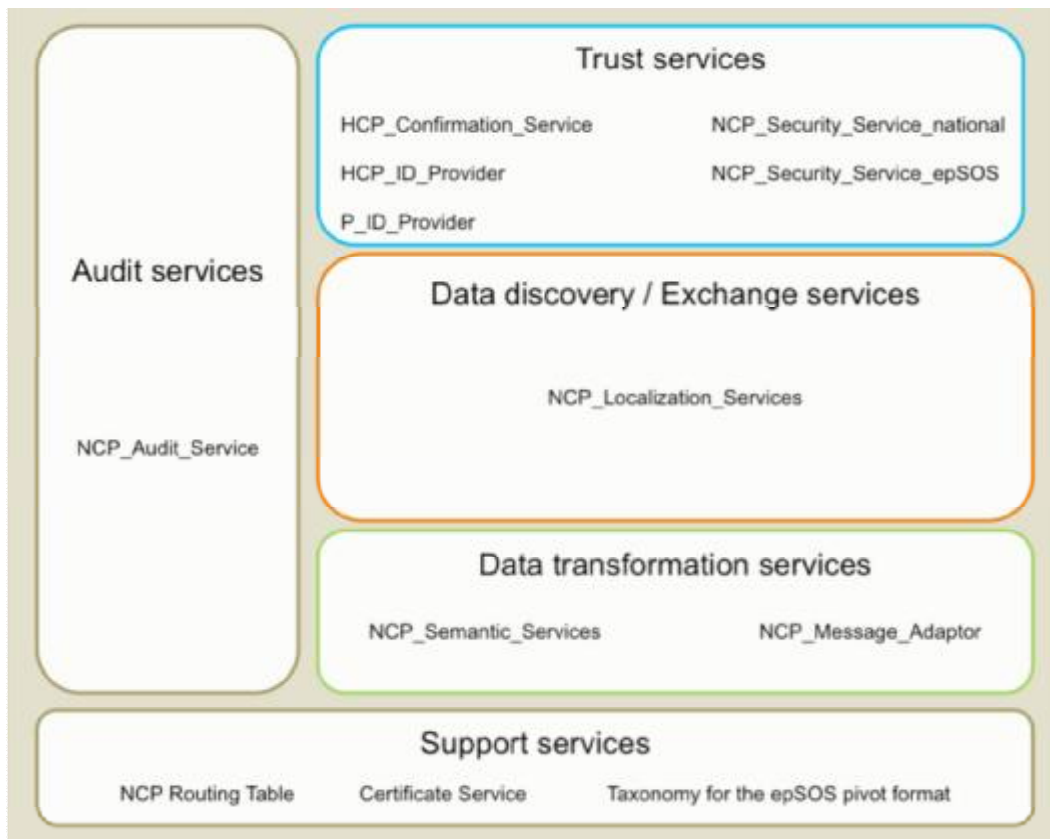


Figure 23: Services "zoning" Overview

5.2.1 Trust – Audit Services

The proposed Information System View, later described in chapter security clearly separates the European security context and the national security context. The separation is realized by the logical component National Contact Point (NCP) which is connected to

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

the epSOS and the National Infrastructure via dedicated interfaces. Each interface has its own network security, own PKI and own semantics as cryptographic standards, taxonomy and messaging. From the epSOS point of view, there is one and only one NCP per Member State (MS) mediating all communication related to the involved MS (see REQ 3.3.3).

According to the description of the NCP functionality, two (security) domains representing the levels of trust have been identified: the epSOS security domain and the national security domain. While the epSOS security domain covers all communication between two NCPs and ensures data protection and privacy, the national security domain ensures the national policies between the NCP and its national gateways. Figure 24 shows the different way to establish End-to-End Trust:

1. Brokering trust by linking security contexts,
2. Pretending End-to-End security by brokering security objects
3. True End-to-End Trust by using End-to-End security objects.

epSOS implements (1) for confidentiality and (2) for integrity and authenticity.

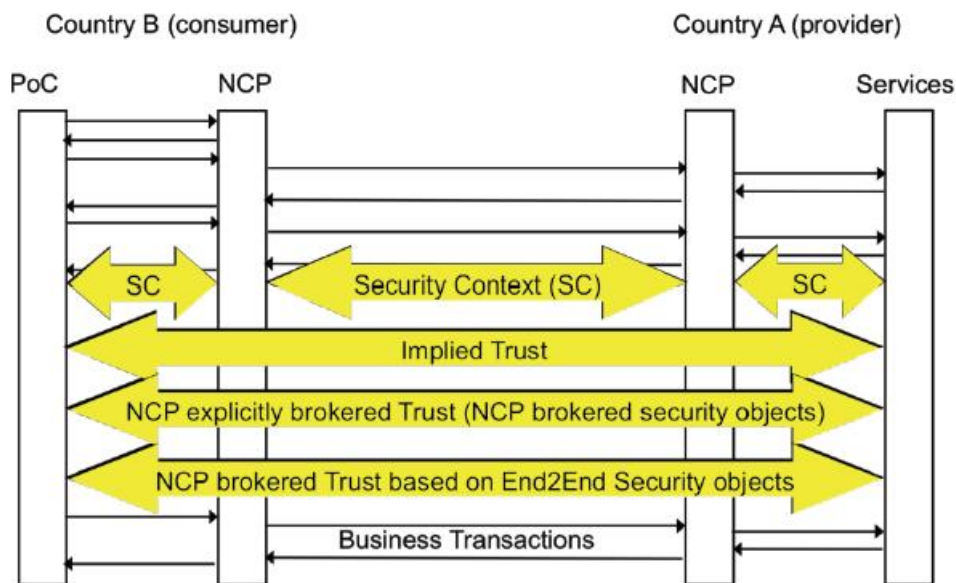



Figure 24: Security Context (“Trust Chain”)

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

epSOS NCPs set up a “Circle of Trust” which is instantiated by the respective communicating gateways. Each NCP as a legal entity guarantees that each communication initiated or accepted by one of its gateways complies with the epSOS security policy, the respective national legislation and all additional agreements among the cooperating countries. It even more guarantees for the integrity and authenticity of its gateways by providing the respective gateway certificates.


The epSOS Circle of Trust defines the actors and transaction for the management and establishment of mutual trust relationships among epSOS gateways and for the operation of a secure channel between these gateways. Thus, it provides a foundation for setting up and maintaining a closed network of trusted nodes on top of an insecure network (e. g. the internet). The Circle of Trust profile makes use of Transport Layer Security (TLS/SSL) to establish connection between country A and country B; and VPN (ipSec) must be used to protect data flows between the 2 NCPs, as well as for signing the SAML assertions (see Chapter “Technology View”).

5.2.1.1 Internal & External Services

Internal & External services are services which are available within the epSOS infrastructure and the interface for the national infrastructure.

- **NCP_Audit_Service:** The service is responsible for auditing of every data access or attempts. There are two aims of auditing, first to satisfy the data privacy law regarding the right of data sovereignty of the patient and second the non-repudiation of origin. It is assumed that the audit trail includes information encoded in epSOS taxonomy in addition to information encoded in national taxonomy. Therefore it is spread over both domains in the model. See epSOS Profile Audit Trail in D3.4.2 on more information regarding the audit process within epSOS.

The component must facilitate the non-repudiation of the actions of every involved party on a technical and organizational level for each and every transaction successfully processed or denied (e.g. prescribing doctor, dispensing pharmacist, NCP routing/mapping, data resource URL retrieval, patient’s identifier query).

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

5.2.1.2 Internal services


Internal services are services residing on the epSOS internal side.

- **NCP_Security_Service_epSOS:** This security service is responsible for the verification and affirmation of integrity, authenticity and confidentiality of each transaction within the epSOS domain (e.g. between NCPs, localization services). Therefore it is able to validate signatures and check the status of certificates that are assigned to its security domain.
- **P_ID_Provider:** This service is responsible for uniquely identifying a patient within epSOS by discovering the unique patient identifier referring to the home community of a patient and the patient identifier that must be used for querying for patient data within that community.

5.2.1.3 External services

External services are services connecting the epSOS infrastructure with the MS' national infrastructure.

- **HCP_ID_Provider:** This service is responsible for providing a unique Id for an HCP within epSOS, which has to be provided by national authorities.
- **NCP_Security Service_National:** This security service is responsible for the verification and affirmation of integrity, authenticity and confidentiality of each transaction within the national domain (e.g. between HCPs and NCP, authorization services). Therefore it is able to validate signatures and check the status of certificates that are assigned to its security domain.
- **HCP_Confirmation_Service:** The component HCP_Authorization_Service provides and controls the consent assertion that is needed to transport the authorization of the HCP by the patient. The authorization process is described in D3.4.2 section 6.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

5.2.2 **Data Exchanges – Data Transformation Services**

5.2.2.1 Internal & External Services

- **NCP_Semantic_Service:** The mapping of medical information and taxonomy is done by the semantic services therefore this component belongs to the internal and external domain. The Semantic Service is described in great detail in D3.5.2. To facilitate a faster implementation we propose the development of an outline for an interface where the most common format is described.

5.2.2.2 Internal services


- § **NCP_Localisation_Services:** The service locates the communication counterpart (NCP-A) and has access to locate tables and maps country IDs to endpoint URLs. It provides the means to discover and access medical resources, while storage is left to national implementation. Localization of data is done via location independent Unified Resource Names (URN), provided by an URN-Resolver, which can be transcribed to URLs referring to the concrete data store.

5.2.2.3 External services

- § **NCP_Message_Adapter:** The adaptation of the national communication protocol is done by the NCP_Message_Adapter, e.g. the splitting of ePrescriptions or the correlation of related messages. It lives in the national domain, because the epSOS internal business logic depends on information provided by the existing national infrastructure.

5.2.3 **epSOS support services**

There are a number of information sources which are relevant for every NCP and must be in the same state for every NCP. Examples for this are common taxonomies, schemas, and WSE addresses of NCPs. This shared data is centrally managed in order to avoid inconsistencies and version conflicts in a generalization process of epSOS.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

Services²¹ are implemented within an NCP by using a static configuration table. It is the responsibility of each NCP to keep the configuration up to date from centrally managed data storage. Each NCP MUST be in charge to manually download new version of any updated data. This operation can be done with a secure method (via SSL, TLS, or SFTP) to upload / download files to and from FTP servers.

5.2.3.1 National Contact Point Routing Table

The Locate central function is a simple NCP Routing Table which facilitates the connections between two NCPs. This service is independent of the form of distribution (e.g; centrally maintained, replicated or locally maintained copies) and can be made available as an XML-document. It is maintained locally. This information is encoded in a NCP configuration file which is specified by D3.4.2. Each NCP MUST hold a copy of the configuration files of all the other NCPs.

5.2.3.2 Trusted Certificates


Certificate services are MS issues. Technical trust in country A is established by acknowledging the certificates that were announced by country B and vice versa after legal trust confirmed.

Certificates from different certificate service providers should be used per communication layer (VPN, TLS, WS-Security).

5.2.3.3 Taxonomy for the epSOS pivot format central function

The Taxonomy central function serves as a library for all existing and valid epSOS pivot formats and all relevant schemas. This information should be robust most of the time and

²¹ Term Service does not mean a web service to synchronise local and remote data, but instead a function link to a manual process for epSOS 2011 pilot. The solution Must be able to turn into a “true” service implementation for next version of EpSOS.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

not to be changed. Therefore this information can be duplicated into each NCP. This should also be relevant for later performance issues.

Each NCP must hold a copy of the taxonomy from a known URL (e.g. www.wpsos.eu/taxon/) where each NCPs can retrieve a copy.

It is the responsibility of each country A to keep the configuration up to date for the NCP.

5.2.3.4 Traits Handshake central function

NCP-A and NCP-B should be able to agree on the identity traits that have to be provided by country B in order to identify a patient. Information on which traits are required for which country are coded within a static client-side configuration. It is the responsibility of each country B client/portal to keep the configuration up to date.

5.3 NCP considerations

As stated before, a national contact point (NCP) is the single legal representative of a Member States' (MS) epSOS services that guarantees the compliance of all the MS' epSOS services with the epSOS information governance. All communication to or from a national health care system of a member state is done through its NCP; direct access to national services MUST NOT be possible (see REQ 3.3.9). Therefore the NCP is the very basic node entity within epSOS.

This logical component can be addressed via two clearly separated interfaces (NCP_IF_National and NCP_IF_EPSOS from figures in chapter 5), each one accessible out of the according network (figure 23). While the concrete implementation of an NCP has to be done by the according member state, the interfaces defined in the chapter Technology View must be served according to epSOS specification.

Underneath the shield of a single NCP a MS may deploy multiple communities where each community is running its own instances of epSOS services to serve the HCPOs, HCPs, and patients that are assigned to the community. Access to a community's epSOS services is mediated through a community gateway that is established as part of the NCP.

Typical examples of communities are regions running their own health services and Cross Enterprise Document Sharing (as agreed XDS Profile) affinity domains as networks of co-operating healthcare enterprises. Countries with centralized health services are assumed to be a single community. Each community is identifiable by a unique ID administrated by the Member State’s NCP.

The next figure shows a conceptual view of the basic NCP architecture. The diagram shows the scope of epSOS and the responsibilities of the NCP.

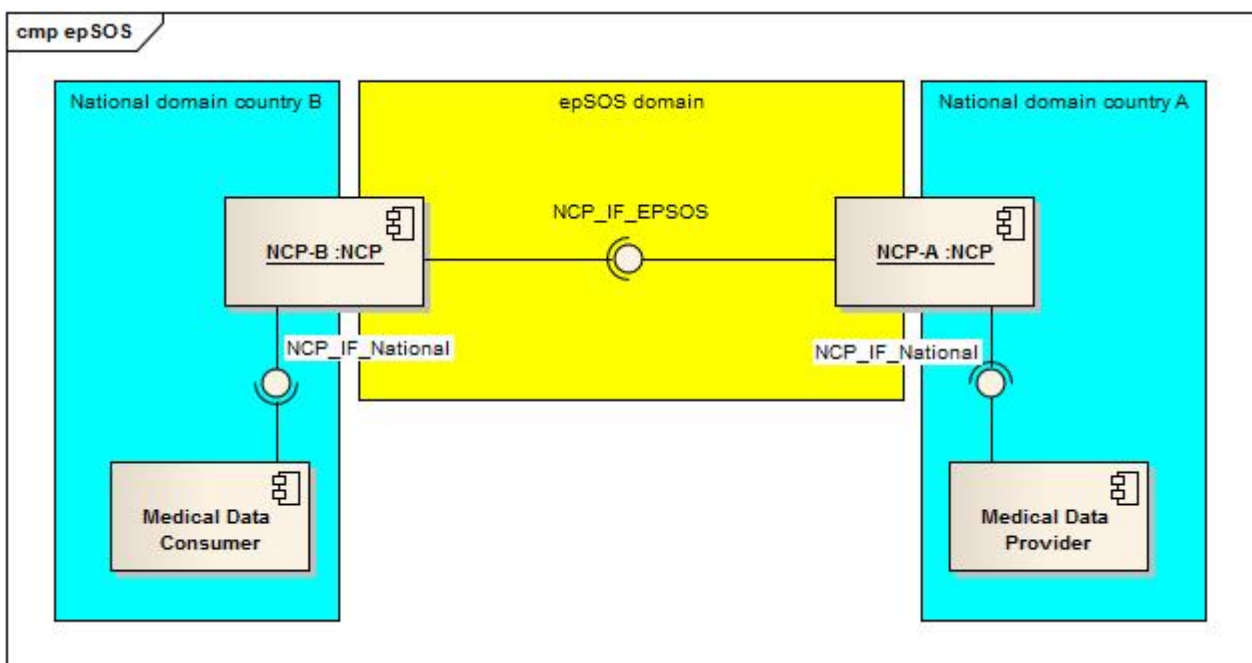


Figure 25: High Level Architecture of a epSOS NCP

The following figure gives a more detailed view on the composition of the NCP. As explained before each NCP works as an interface between the national infrastructure of the MS and the epSOS domain. Each NCP hosts services which work in different contexts and have strongly separated responsibilities.

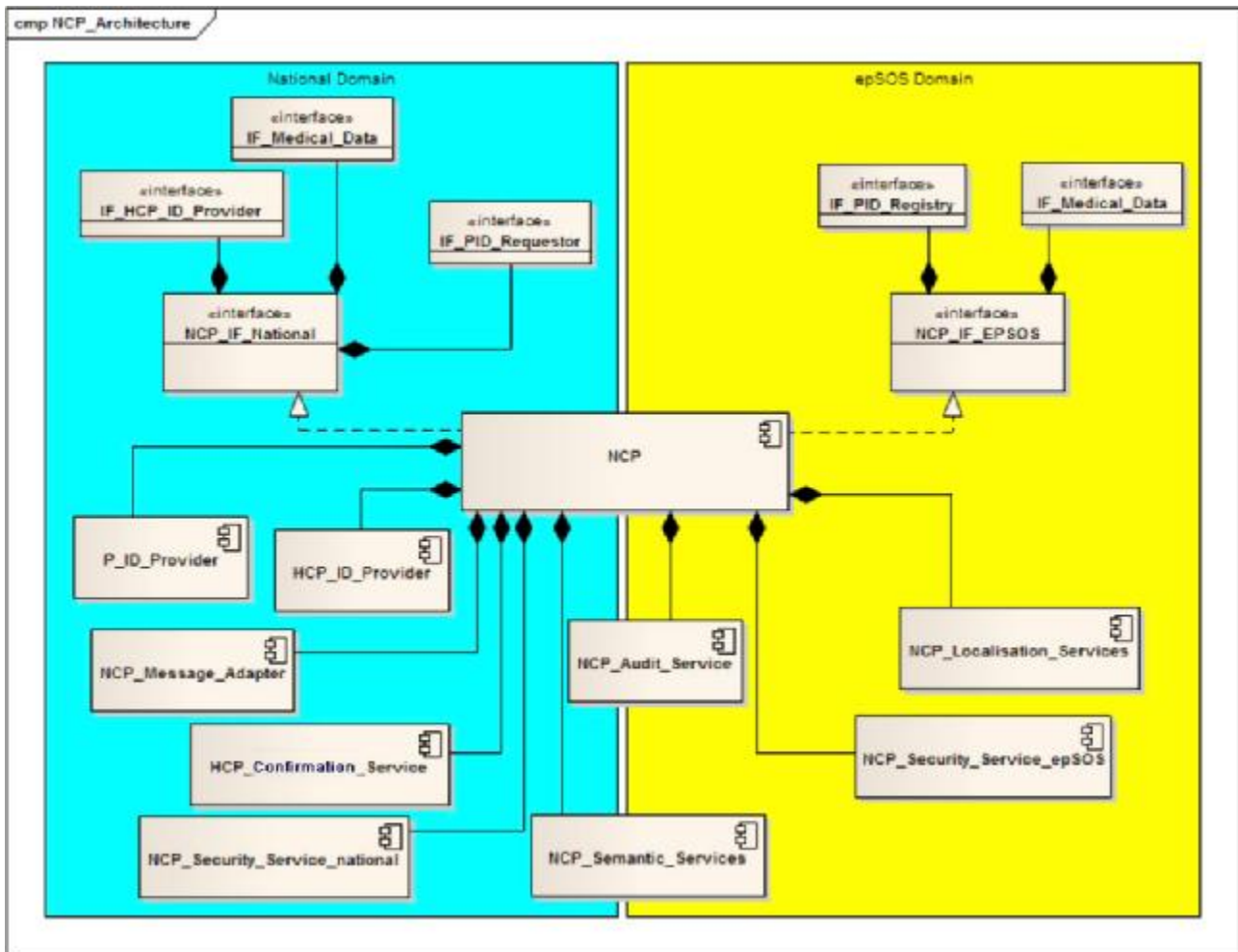



Figure 26: Detailed Composition of NCP components

5.3.1 NCP Interface to national domain

The interface that connects the NCP to the national network (NCP_IF_National) is composed of the sub interface to request a patient ID (IF_PID_Reqestor), the sub interface that is used for the applications ePrescription (eP) and Patient Summary (PS), both served by IF_Medical_Data and the sub interface that is used to request a HCP identity assertion (IF_HCP_ID_Provider). Processes and components beyond the interface that connects the NCP with the national infrastructure (NCP_IF_National) are not part of the epSOS specifications.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

5.3.2 *NCP Interface to epSOS domain*

The interface that connects the NCP to the epSOS network is composed of two sub-interfaces, the interface that is used to query medical data (IF_Medical_Data) and the interface that is used to query PID information (IF_PID_Registry).

5.4 Security considerations

Since epSOS deals with medical data, there is a need to implement strong security mechanisms to ensure the authenticity, integrity and security of this data. The basic security principle in epSOS is the “circle of trust”, which means that each and every NCP trusts its peers from other MS. In addition to this basic principle, several additional security services are needed to provide the necessary level of security. For a more detailed description of these services see D3.7.2.

The security services are the following:

1. Access control: It MUST be ensured that only authorized HCPs can retrieve data from epSOS. Each NCP is responsible for accepting or rejecting an authorization request of a HCP of its MS. For all NCPs are to trust each other an HCP only needs to authenticate at the NCP of his MS. Data exchange MUST follow the national law of the involved MS. Implementation lies in the responsibility of the involved NCPs of the MSs. It MUST be ensured, that the data transmitted within epSOS stays intact to ensure the safety of the patient.
2. Data Confidentiality: Since medical data is a highly sensible data it MUST be ensured that no unauthorized party is allowed access to this data.
3. Non Repudiation: Non-repudiation of origin MUST be ensured by each NCP. It therefore logs every transmission and the involved parties (see auditing services) and enables signing and encryption mechanisms not only between NCPs but also between HCP(O)s and NCPs.
4. PKI: For the certificate management a PKI is needed which acts as a CA and administrates a list of trusted epSOS certificates and a revocation list.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

5. Auditing and Accounting: Each NCP logs each and every data access (and every party accessing the data) via its interfaces. For proper traceability this service includes a time service synchronizing all NCP-clocks.

5.5 Information Objects

This chapter comprises data objects administrated by the NCP. The following figure gives an overview of the necessary business objects and their relation. These objects are more closely described in course of this chapter.

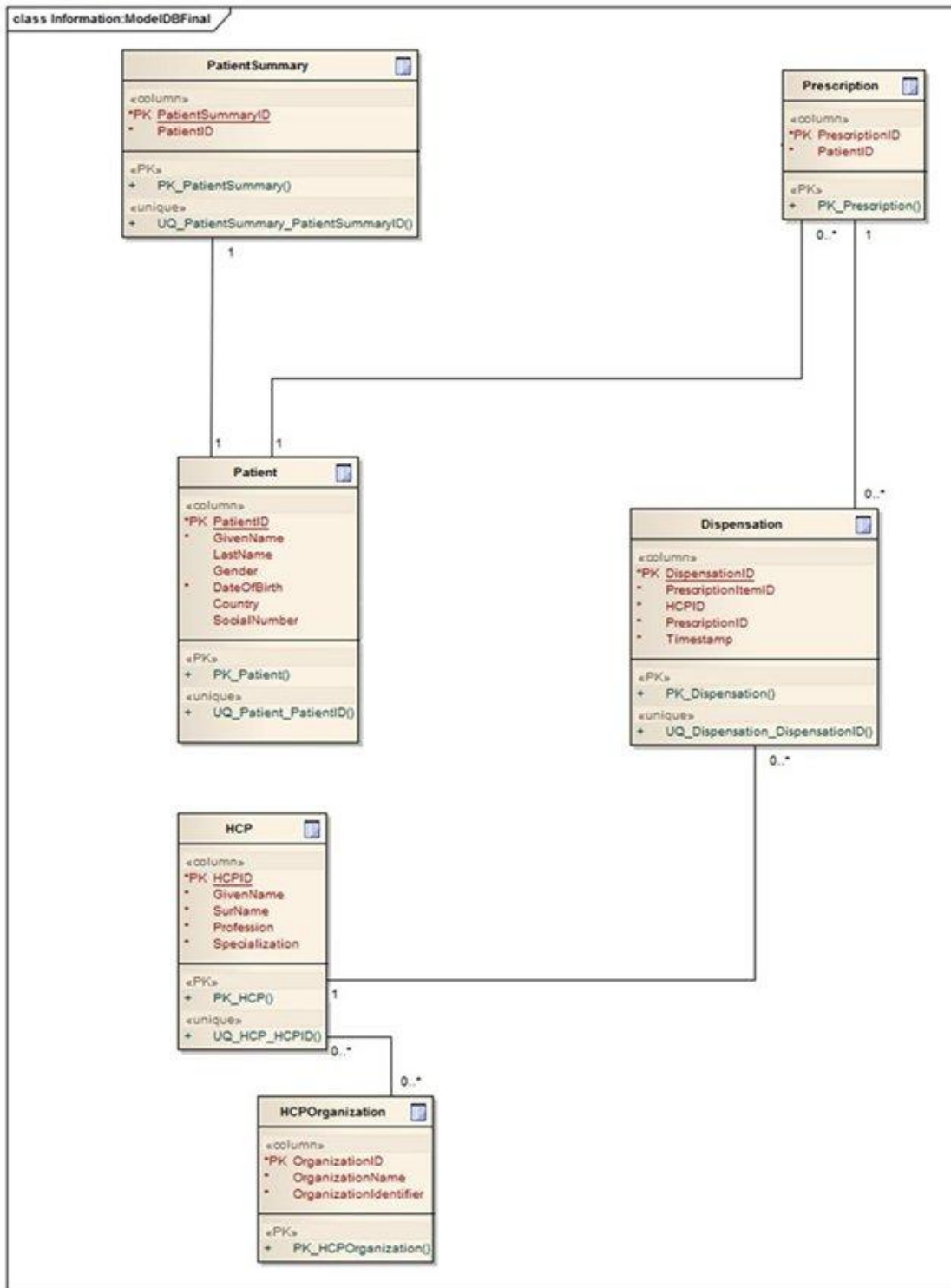



Figure 27: Schematic representation of the Data Objects and their relations

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

5.5.1 **Health Care Professional (HCP)**

A health care professional is a physician participating in epSOS identifiable by its unique id. It is affiliated to zero or more health care professional organizations, depending on national legislation.

The HCP contains information as defined in D3.1.1. A HCP is related to 0..n HCPOs and is associated with 1..n Healthcare Professional Addresses.

5.5.1.1 Healthcare Professional Address

The Healthcare Professional Address object contains information defined in D3.1.1. An Healthcare Professional Address is related to 0..n HCPs. Since an Healthcare Professional Address can be in the system, even though an HCP is removed from the epSOS context, this address doesn't necessarily have to be deleted, therefore an address belonging to no HCP SHOULD be allowed.


5.5.1.2 Health Care Professional Organization (HCPO)

A Health Care Professional Organization is a logical entity within the national environment known to the NCP and uniquely identifiable by its id.

The HCPO object contains information defined in D3.1.1. An HCPO is related to 1..n HCPs. At any given time in the context of an epSOS transaction, an HCP MUST be associated with only one HCPO.

5.5.2 **Patient**

A patient is an individual person participating in epSOS by giving permission (prior consent) in his home community to process his/her medical data to a foreign member state. Within his home country each patient is assigned to a single community that can mediate access to that patient's PS and ePrescriptions. This community is called the patient's home community. It may be possible that, in future projects based on epSOS,

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

data of each patient is being managed in multiple communities but this scenario is out of scope of epSOS


For participating in epSOS the patient has to give within his home community his permission (consent) for the usage of his data by epSOS (prior consent). Additionally the patient has to give its permission for the actual usage of its data in the foreign MS by explicitly authorizing a health care operator to do so (activation of an existing consent). Alternatively the involved HCP in MS B may request an emergency access to the patient's data (e.g. in case the patient is not responsive). This access has to be handled by the NCP in regard to MS A's legislation (MS A can accept or decline this request). D3.4.2 describes the management of the patient's consent in great detail.

The Patient object contains information defined in D3.1.1. A patient MUST be related to 0..1 PS, 0..* ePs and 0..n eDispenses.

5.5.3 *Patient Summary (PS)*

The patient summary contains the patient's medical information. The patient summary may also include the medication summary. As previously stated every access to the patient summary and ePrescription data is read only²². There will be no write access to this data within epSOS. Figure 28 shows the lifecycle of a PS within epSOS. The PS is available if the patient has agreed to take part in epSOS, and is not available if the patient decides not to take part in epSOS anymore.

²² Actually, patient summary and prescription data are provided through services, therefore the actual national database is not accessible directly.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

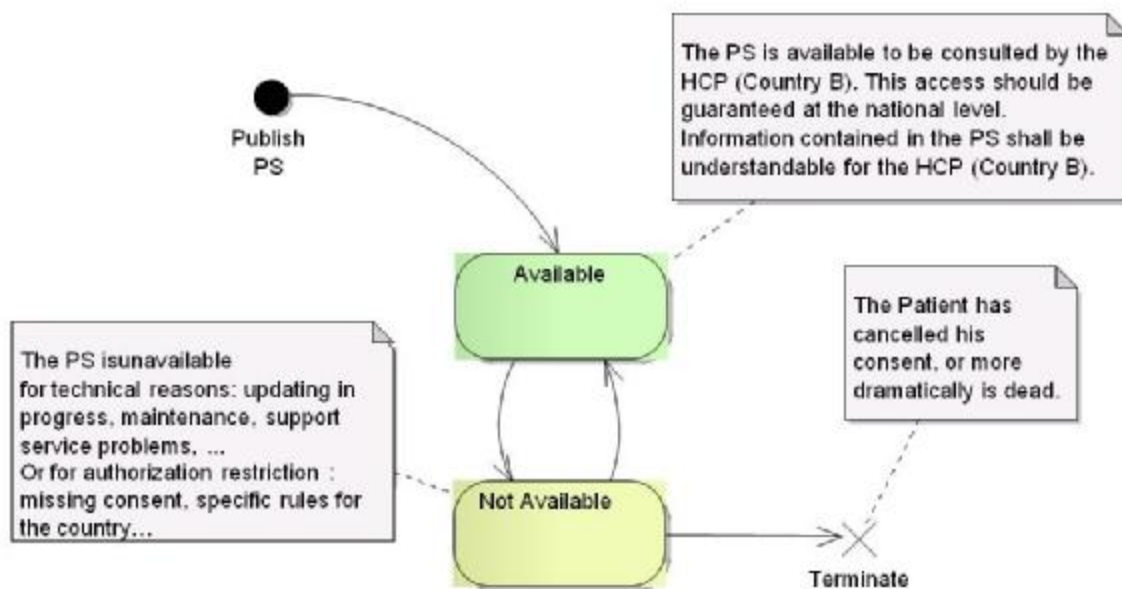


Figure 28: Life cycle of the Patient Summary

The PS object contains the information about the patient as defined in D.3.2.1. Every PS MUST be related to exactly 1 patient.

5.5.3.1 Medication Summary

The Medication Summary is not requested as an OPTIONAL part of the PS, but it is left to Member State the responsibility to define mutual agreement for Medical Summary

5.5.4 **ePrescription (eP)**

The eP object contains information about the medicine prescribed in MS A. The status management of the eP is an internal MS affair (i.e. it may differ from country to country) and D3.1.2 does not give specifications for this topic. The minimum basic status is “Available” or “Not Available” as presented for the Patient Summary.

Figure 29 shows a **suggested** lifecycle for an eP. When looking at the lifecycle the following states can be reached by an eP:



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

1. Ordered: This state is reached when the prescriber has written the eP and the eP is included in the patient's electronic health record (EHR).
2. Placed: This state is reached when the ordered eP has been recorded into the national/regional eP service and is now ready to be accessed by the dispenser.
3. Cancelled: This state is reached if the eP is invalidated before dispensed completely.
4. Suspended: If an eP can be dispensed more than one time and requires a certain time span between dispersions, the eP assumes the state Suspended in this time. It reaches the state Partially dispensed when the eP becomes available again.
5. Partially Dispensed: If a single ePrescription contains multiple items -or items which can be multiply dispensed - it reaches this state if the eP is not dispensed completely.
6. Completed: This state is reached when all ePrescription items have been fully dispensed.
7. Closed: This state is reached if the eP loses its validity before it has been fully dispensed (e.g. the eP's time validity has run out, or the patient has withdrawn consent).

A ePrescription with a given consent is valid for the duration defined by MS A and may contain multiple ePrescription Items which may not all be dispensed in one transaction. The object must contain the information defined in D3.1.2. An eP MAY include multiple but MUST include at least one ePrescription item. Every eP is related to exactly 1 patient.

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

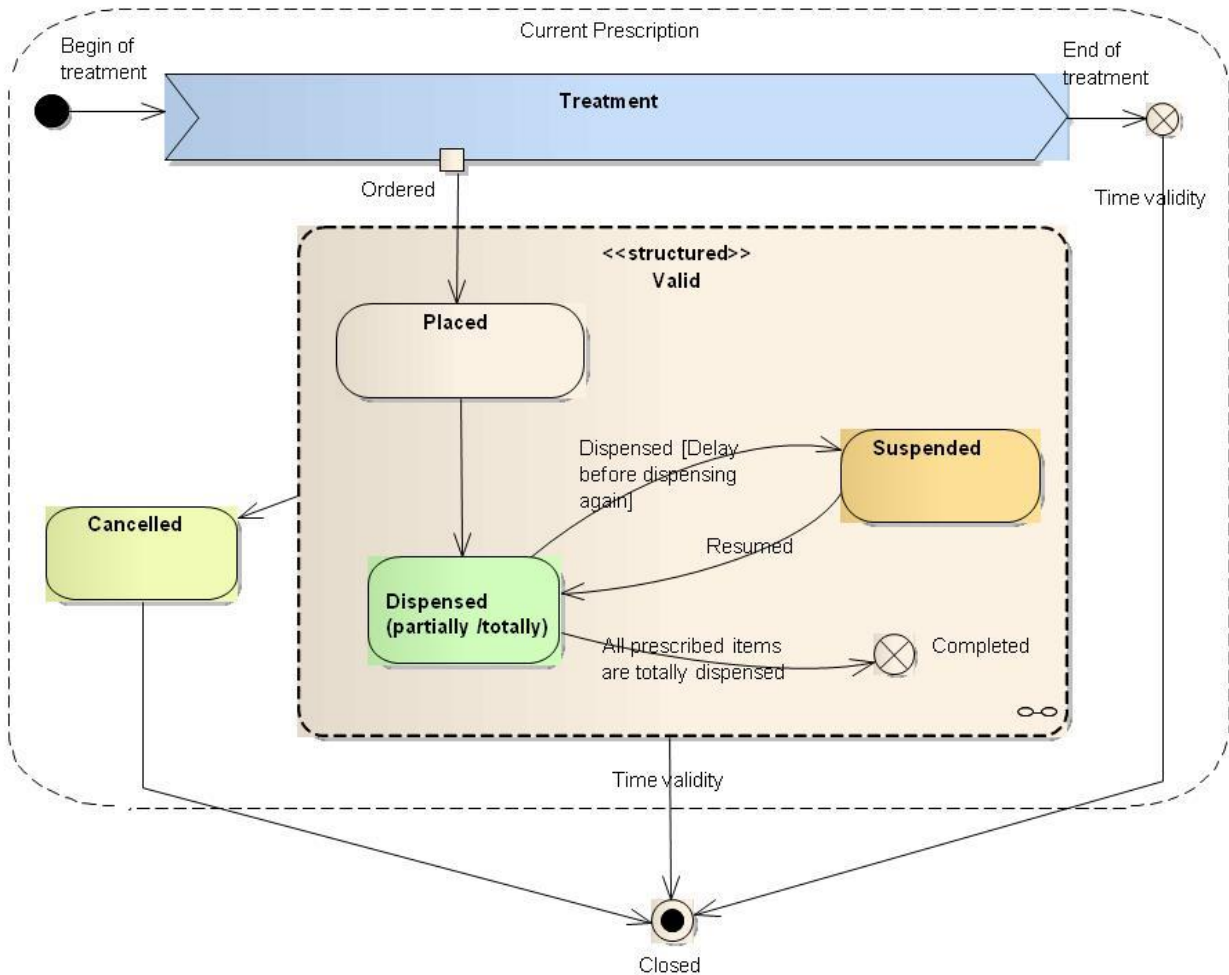


Figure 29: Suggested Lifecycle of an ePrescription

5.5.5 eDispense

In epSOS the event of a patient's eDispense is handled via a notification message from MS B to MS A. MS A has to decide how to handle the eDispense event. Since an ePrescription may contain multiple ePrescription items, it must be possible to allow multiple eDispenses for one ePrescription. There are two ways for the NCP to handle multiple eDispenses (for details see D3.4.2):

- § If not all eP Items have been dispensed as seen in the notification, generate a new eP containing only the non-dispensed medicines. This is a task of the HCPO. Nevertheless, according to every MS legislation, this option may be implemented at the NCP level.




D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

§ If not all ePrescription Items have been dispensed, return the original ePrescription again and raise an error if a notification is received on an already dispensed medicine. This requires that the pharmacists MUST wait for the result of the notification before the pharmacist can dispense the medicine to the patient.

The eDispense object contains information about a dispensed eP as defined in D3.1.1. A Dispense MUST be related to exactly one dispensing HCP.

Service	Internal	External	Data Object	Document
<i>NCP_Audit_Service</i>	X		<i>Health Care Professional (HCP)</i>	D3.1.1
<i>NCP_Security_Service_epSOS</i>	X		<i>Health Care Professional Address</i>	D3.1.1
<i>NCP_Security_Service_National</i>		X	<i>Health Care Professional Organization (HCPO)</i>	D3.1.1
<i>HCP_Authorization_Service</i>			<i>Patient</i>	D3.1.1
<i>NCP_Semantic_Service</i>	X		<i>Patient Summary (PS)</i>	D3.2.1
<i>NCP_Localisation_Services</i>	X		<i>Medication Summary</i>	D3.2.1
<i>NCP_Message_Adapter</i>	X		<i>ePrescription</i>	D3.1.1
<i>P_ID_Provider</i>	X	X	<i>Dispense</i>	D3.1.1
<i>HCP_ID_Provider</i>	X	X		

Internal Services at National level are not described in this document. The D3.3.2 document does not aim at changing the National Infrastructure and does not provide any guideline for this task. Internal Service presentation is only presented to ease the comprehension of the whole NCP. The National Connector MUST wrap Internal Services.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

This document proposes the interface for the National Connector as it is described in the Technology View chapter (components description), not its implementation.

At the other hand, Internal Services are technically described, starting with the next chapter: Technology View.

6. Technology View

The scope of this chapter is to give the webservices stack view of epSOS in order to build systems and infrastructures needed for operations. This chapter is addressing:

- § The description of services and its external interface,
- § The mapping of transactions and profiles with identified services and interfaces.


On this basis, the intent of this chapter is to help the Member States completing their own call for tender in order to prepare the pilots.

Obviously, the present chapter is closely related to D3.4.2 “epSOS common components” describing epSOS profiles, actors and transactions. Reader can also refer to D3.3.3 (Interoperability Framework) for a cross-reference of standards and protocols used by the various epSOS Profiles.

6.1 From Information System view to Technology view

The primary reason for developing technological view is to support the application by providing the fundamental technology and solution for epSOS: Information system view on the previous chapter needs to get implemented. To do so, epSOS profiles – acting as basic unit manipulated in the architecture - are integrated.

Furthermore, the Technology View details the structure and relationships of the technical services provided by the Gateways, how the components will work, and how technology will support the epSOS’s application goals. This makes a responsive asset for a successful technological model. The technological view addresses this need, by providing

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

a context of the system in response to the changing needs for the data PS and eP exchange environment.

Finally, the Technological View enables to achieve the right balance between efficiency and requirements. In essence, it aligns the epSOS business view and system information view. At the same time, it assures the needs of the composition for integrated components, permitting the closest possible definition for the future Large Scale Pilot.

6.2 epSOS platform

6.2.1 Foreword


The epSOS platform aims to allow the “pan-European health data exchange in a regular and easy manner without changing existing national healthcare infrastructures and legislations, within a trust framework (contracts and agreed policies) among Member States”. This task is accomplished through a Business-to-Business cooperation of a set of national gateways (the technical embodiment of National Contact Points) under a mutual circle of trust.

The notion of platform in epSOS context must be applied with some careful specification. The term “platform” is inherently relative and it's quite evident that epSOS WP3.3 documents must not specify single normative solution architecture. Further investigations have been dedicated to the WP3.8-3.9 Joint Work Group (JWG).

For this reason, the epSOS architecture has its specific “normative” platform model in “service space”. The choice at this level is the WS* stack and some supporting eHealth standard and open specification.

However, some architectural definition is outlined in a Platform Independent flavor²³: epSOS gateway “internal” components architecture can be implemented with different specific low-level technology platform.

²³ With “Platform Independent Model” and “Platform Specific Model” we make an explicit reference on a Model Driven terminology (see www.omg.org/mda)

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

6.2.2 epSOS Domains

The following figure illustrates the different domains of epSOS outlined in Chapter “Business View”. Domains categorize those capabilities:

§ National infrastructure (National Infrastructure of HCP and HCPO)

§ National communication layer

§ Business layer

§ epSOS communication layer

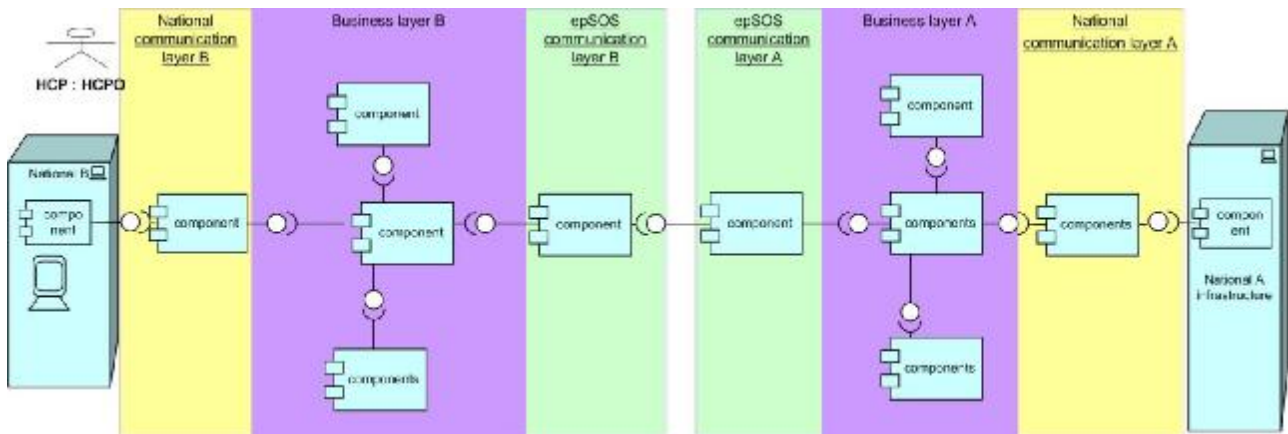


Figure 30: epSOS domains view

This does imply technically:

6.2.2.1 epSOS communication layer

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



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

6.2.2.2 Business Layer

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

6.2.2.3 National communication layer

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


6.3 epSOS Technical Architecture

6.3.1 **Introduction**

The epSOS platform model can be viewed as federations of services connected via specified contracts that define their service interfaces. The resulting system design is a Service Oriented Architecture (SOA).

For the epSOS basic goal of interoperability, SOA is a relevant architectural style: it can decouple interface and implementation as well as avoid dependence or future rigidity. In an SOA solution, the only characteristic of a service that a requesting application needs to know about is the “public” interface. Member States can decide to run the business logic under different operating environments, with different languages and framework or different internal solution architecture.

As defined previously the normative technology platform for epSOS SOA is the web services stack.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

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. The federation of NCPs is implemented via a »circle of trust«.

6.3.2 **Service Architecture**

Capabilities required by the epSOS project are implemented through the architecture described hereafter. SOA is an architecture that enables business agility through the use of common services. 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 (WSDL not in this document, see D3.4.2). 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 inquiries from the service consumer.

The communication between service consumer and services provider is synchronous. The service consumer's control flow is disrupted 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.

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

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

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.

This figure below represents the collaboration among the participant of epSOS Service Architecture²⁴. Along with the UML stereotype «ServiceContract», the main service contract is represented: it defines the interface provided and consumed by the main components (participants).

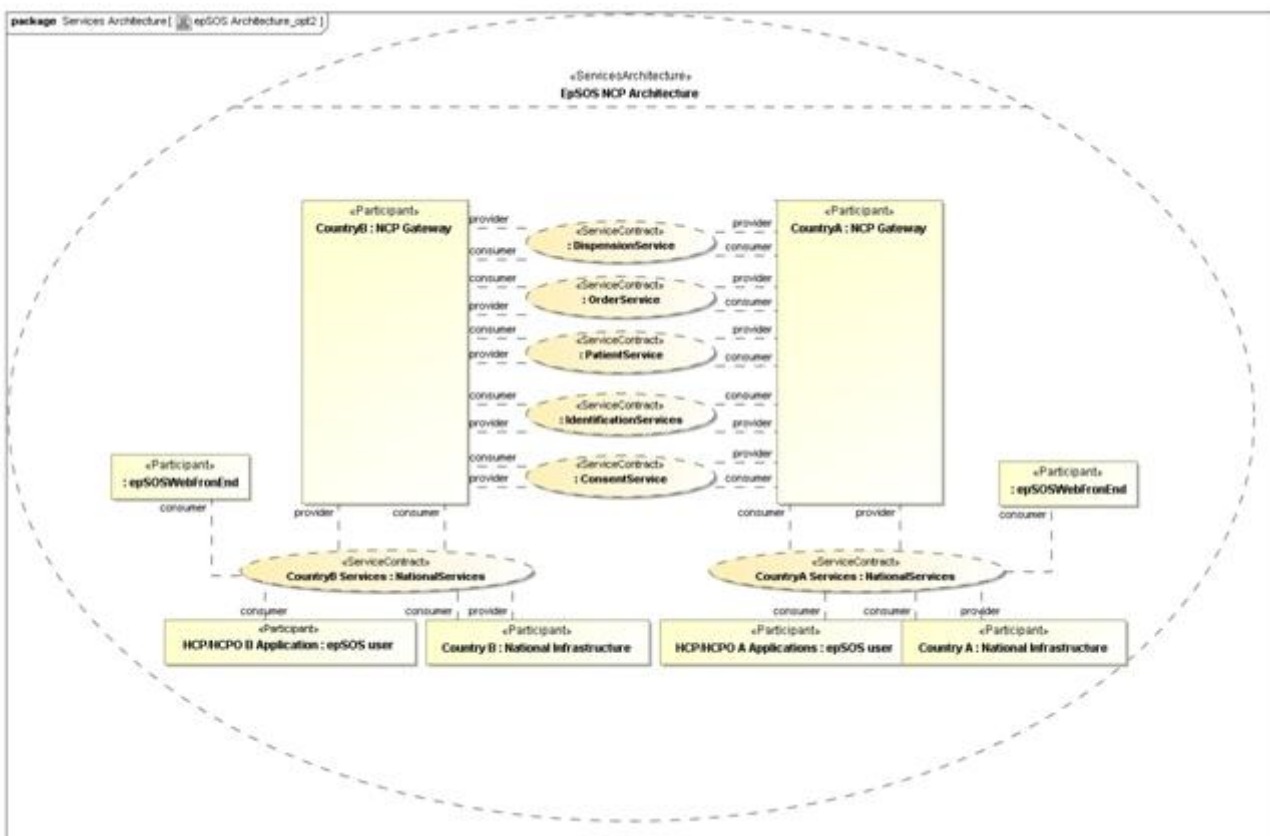



Figure 31 : Core epSOS technical service architecture

²⁴ The representation makes use of UML profile for Services (SoaML, see <http://www.omgwiki.org/SoaML/doku.php>).

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

Moreover Gateways interact with the National Level as well through National Services, in order to allow national infrastructures to get the epSOS capabilities, which is the resulting action of epSOS.

The epSOS Gateways interacts externally towards the epSOS network for these purposes:

- § The exchange of eP, PS and eDispense documents is implemented respectively with **OrderService**, **PatientService**, **DispensationService**, **ConsentServices** service contracts.
- § The Patient Identification is done with the service **IdentificationServices**. Regarding this service, Gateway plays both a consumer and provider role.
- § Operating system (e.g. Linux) enables to configure *time synchronization* for epSOS.
- § Extra inner/outer Services inside of the gateway such as security, transformation, external and internal communication will be described along the following chapters.

NB:

- § *Security concerns are not mentioned in this schema but are detailed further in the chapter Security.*

The epSOSWebFrontEnd Portal component is part of WP3.8 specifications.

But the epSOSWebFrontEnd Portal component remains the member states decision according to their existing architecture²⁵.

Only requirements from WP 3.4 and WP 3.3 with a “MUST” have to be respected strictly by Member State.

²⁵ This component is an implementation of a UI Mediator pattern (http://www.soapatterns.org/ui_mediator.php see Thomas Erl, *SOA Design Pattern*, Prentice Hall, 2009). The epSOSWebFrontEnd in this way establish mediator logic responsible for ensuring timely interaction and feedback with user-interfaces and presentation logic.

The details about these services interfaces are described in chapter 6.5, following the components and composite structure description.

6.4 Composite Structure

In this section the link between services and technical components describe the composite structure.

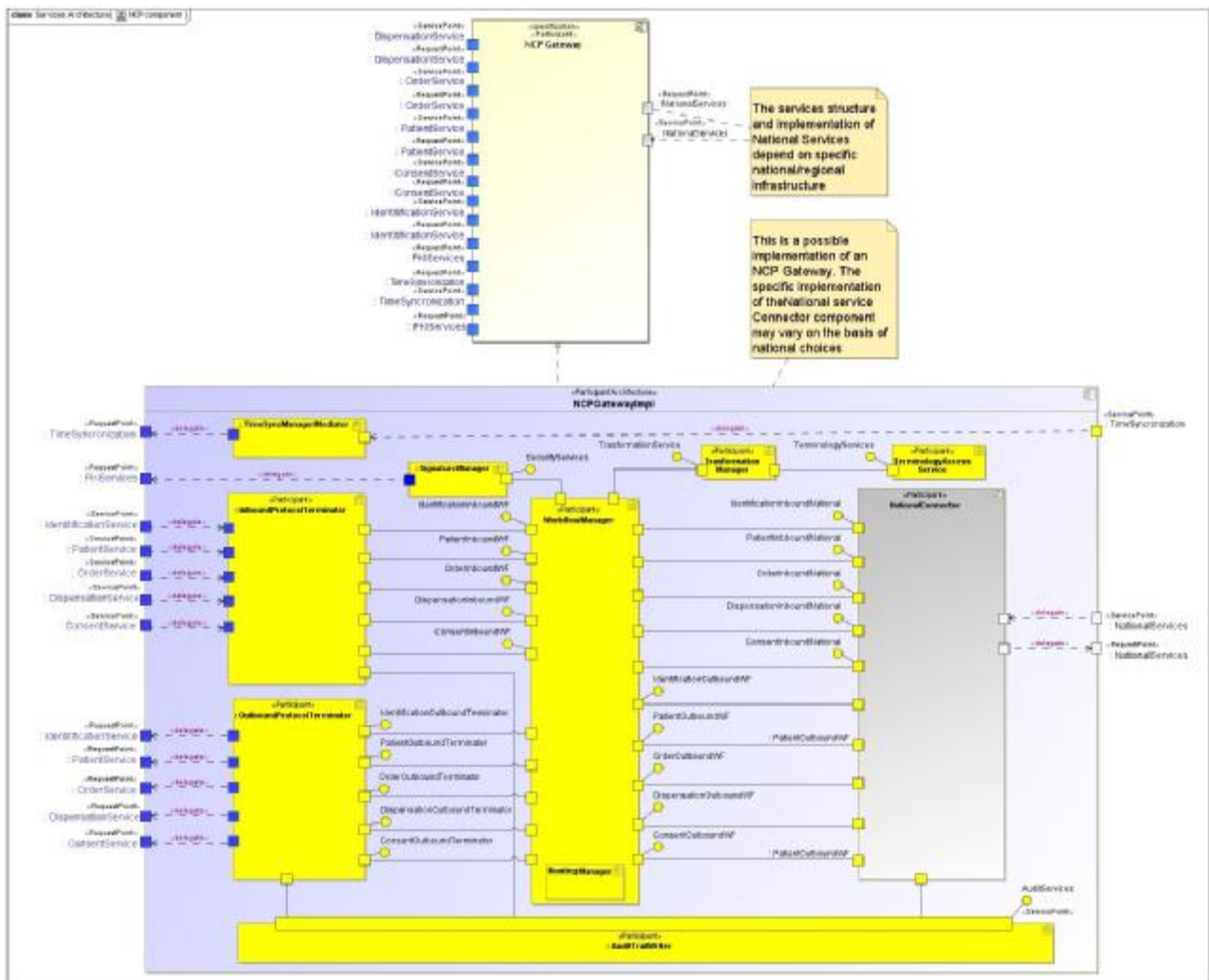



Figure 32: Composite Structure of the NCP Gateway Implementation

This figure represents an implementation of the NCP. Any other implementations would remain possible as long as all the business functional requirements are respected. For

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

instance, the WorkflowManager component is not mandatory, but the business operations associated to the Manager are mandatory.

NCP Gateway implementation component offers service and request ports both to the epSOS network (“normative” interfaces) and to the National Infrastructure (country specific interfaces).

The gateway internal structure is organized to accept/send messages from other NCPs with the InBoundProtocolTerminator/OutBoundProtocolTerminator. The WorkflowManager acts as a controller and composes the flow between others component. The SecurityManager is under the control of the WorkFlowManager, as it is for the TransformationManager.

The dedicated task to communicate with the National Infrastructure is done by the NationalConnector.

Note: The internal composition of the NCP has been designed to be deployed, to any National Infrastructure. JWG WP 3.8 is in charge to define the NCP common components.

6.4.1 **Components Description**

All the mentioned services are implemented through the NCP gateway under the following layers.

6.4.1.1 The National Communication layer

- § The InboundProtocolTerminator acts as the entry point for any epSOS messages, it adapts the entry to the inner components like the WorkFlowManager
- § The OutBoundProtocolTerminator plays the opposite role of the InBoundProtocolTerminator by adapting messages from inner NCP components for other NCPs.

6.4.1.2 The Business Layer

- § The SecurityManager is a guarantor for epSOS protection and integrity.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

- § TheTransformationManager turns epSOS pivot into national schema and vice versa.
- § The TerminologyServiceAccessManager is translating a given concept designation into the requested target language as well as transcoding a given “local” coded into the appropriate epSOS coded.
- § The WorkflowManager, as a role of a controller which does interact with other components (e.g InboundProtocolTerminator). It helps the structured implementation for the pilot, inspired by the MVC IT pattern.²⁶
- § The RoutingManager resolved routing to the corresponding NCP

6.4.1.3 The National Communication Layer


- § The NationalConnector is in charge to link Business NCP components to the national Infrastructure. Authentication and authorization service for local HCP is included in the NationalConnector.
- § A PolicyManager can be added is needed, but for a sake of simplicity it is not include in the figure “Composite Structure of the NCP Gateway Implementation”. See WP3.4 and 3.7 for detail about PolicyManager.

6.4.1.4 The Platform layer

- § ConfigurationAndMonitoringManager manages configuration and monitors components.
- § The Audit Trail support epSOS all transactions that must be audited (other component such as AuditTraitsRepository can be added).

More details about these components are provided in the WP3.8 & WP3.9 JWG NCP HLDD common components documents.

²⁶ <http://en.wikipedia.org/wiki/Model%E2%80%93view%E2%80%93controller>

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

How these components interact to support the Data Exchange and the Patient Identification scenarios are described in Section Component Communication.

NB: An authentication and authorization service for local HCP is included in the NationalConnector.

6.4.2 **Components Description**

§ *Components are part of the starting epSOS platform for service orientation throughout software engineering. They are often mapped with services able to fulfil epSOS requirements.*

§ *In the following text, DocumentID is considered to be an OID (Object Identifier) such as required by WP3.4 and WP3.5.*

§ *HCP identification/authentication and consent confirmation (or Treatment Relationship confirmation) implementation is left to MS but SAML assertion is required for safeguarding business requests.*

6.4.2.1 *Inbound Protocol Terminator*

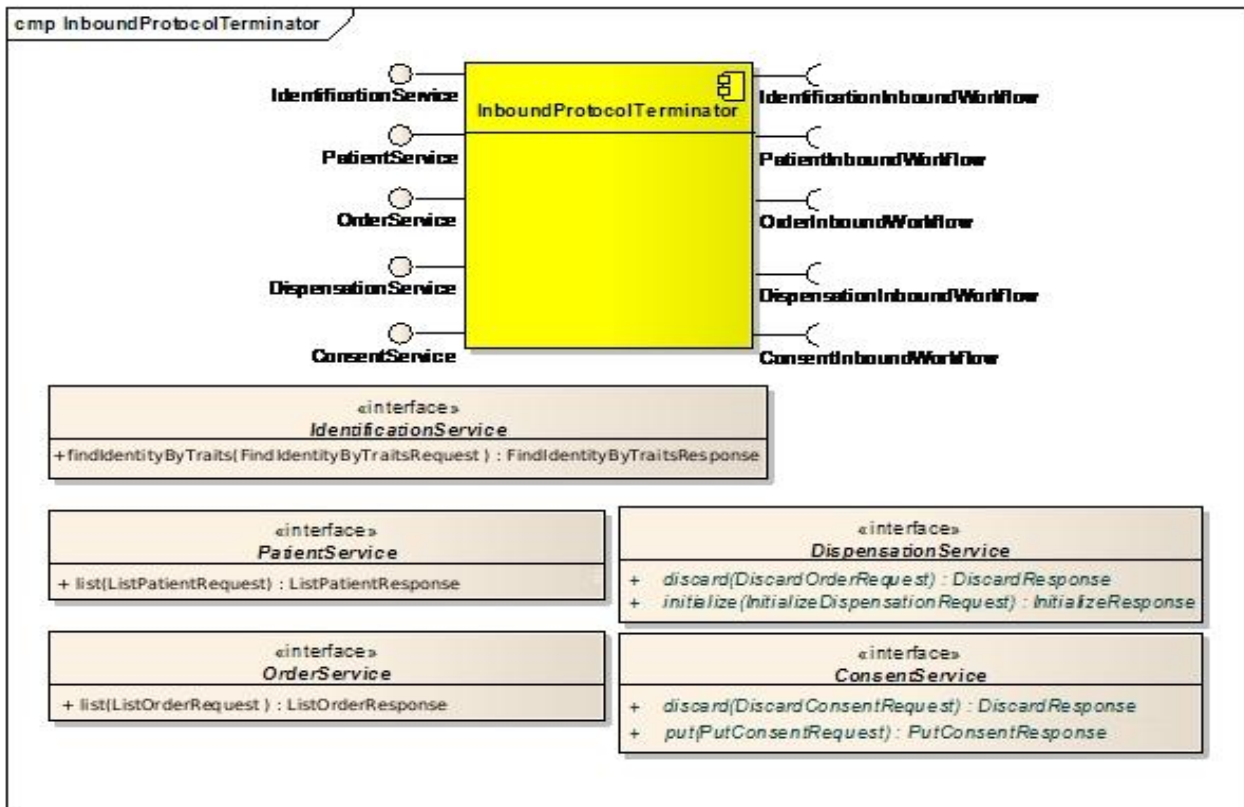


Figure 33: Inbound Protocol Terminator

The InboundProtocolTerminator is the entry point for an EpSOS message arriving in the NCP. The InboundProtocolTerminator component plays the role of a service provider SOAP web services for other NCPs. The InboundProtocolTerminator performs verification of WS-Security SAML tokens and deserializes SOAP message into objects for the use of WorkflowManager. It adapts messages to the components inside of the NCP.

WebService implementations provided by the InboundProtocolTerminator are the following:

- § PatientIdentificationService
- § Patient Service
- § Order Service
- § Dispensation Service
- § Consent Service

The InBoundProtocolTerminator renders the epSOS medical data into a form suitable for the WorkFlowManager,

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

6.4.2.2 *Outbound Protocol Terminator*

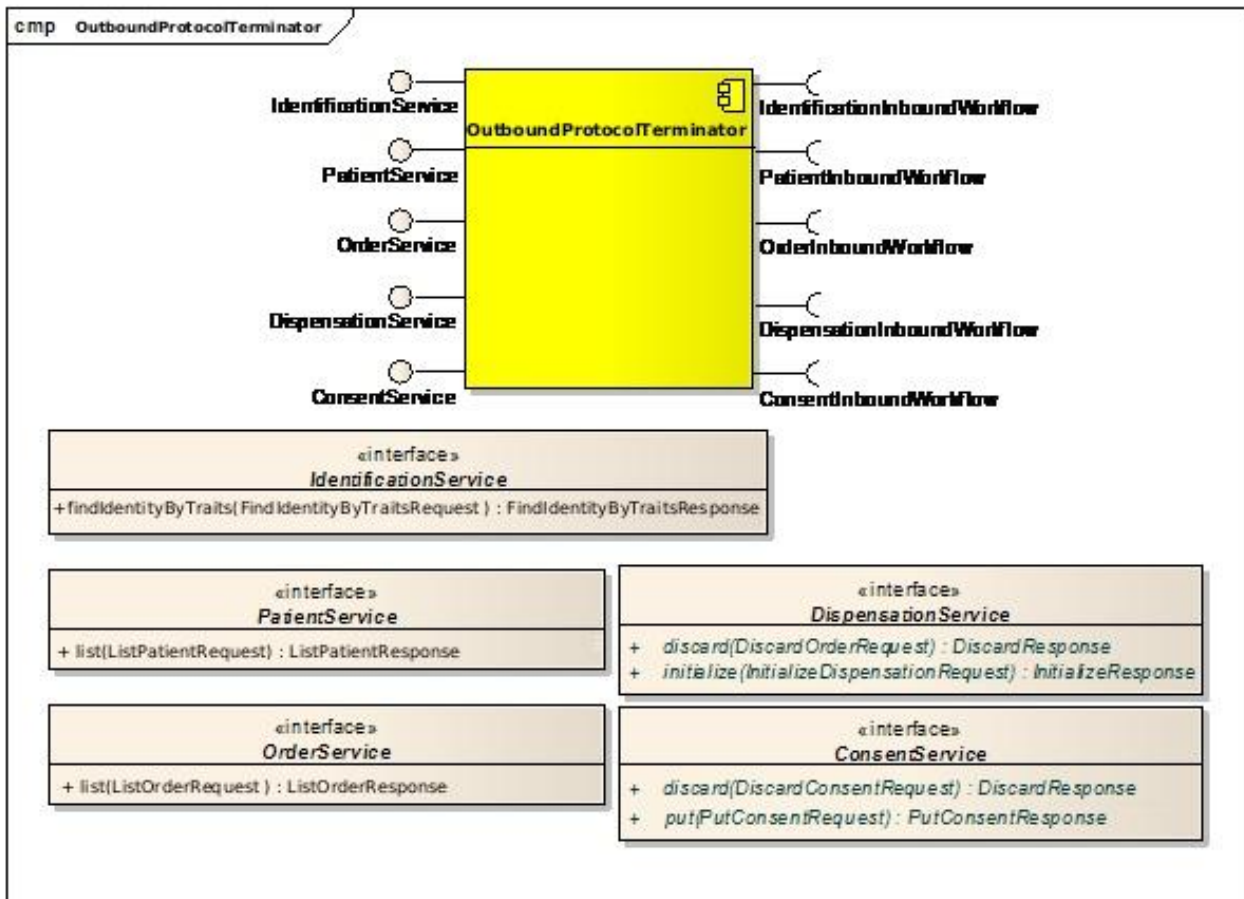


Figure 34: Outbound Protocol Terminator

The OutboundProtocolTerminator plays role of a service consumer. It serializes message objects in a SOAP request, adds corresponding WS-Security tokens and routes it to the NCP addressed by the country of affiliation of the patient. When the response arrives, it performs the deserialization of the SOAP response into object instance for the use of the WorkFlowManager. The OutboundProtocolTerminator is able to communicate over the network to other NCPs, because it is a consumer, it acts as a client and can query services located to the InboundProtocolTerminator. Even if this component is not needed for a business purpose, it realizes the adaptation of messages. With the ProtocolTerminators epSOS get a structured organization for a dedicated task to a specific component.

6.4.2.3 Workflow Manager

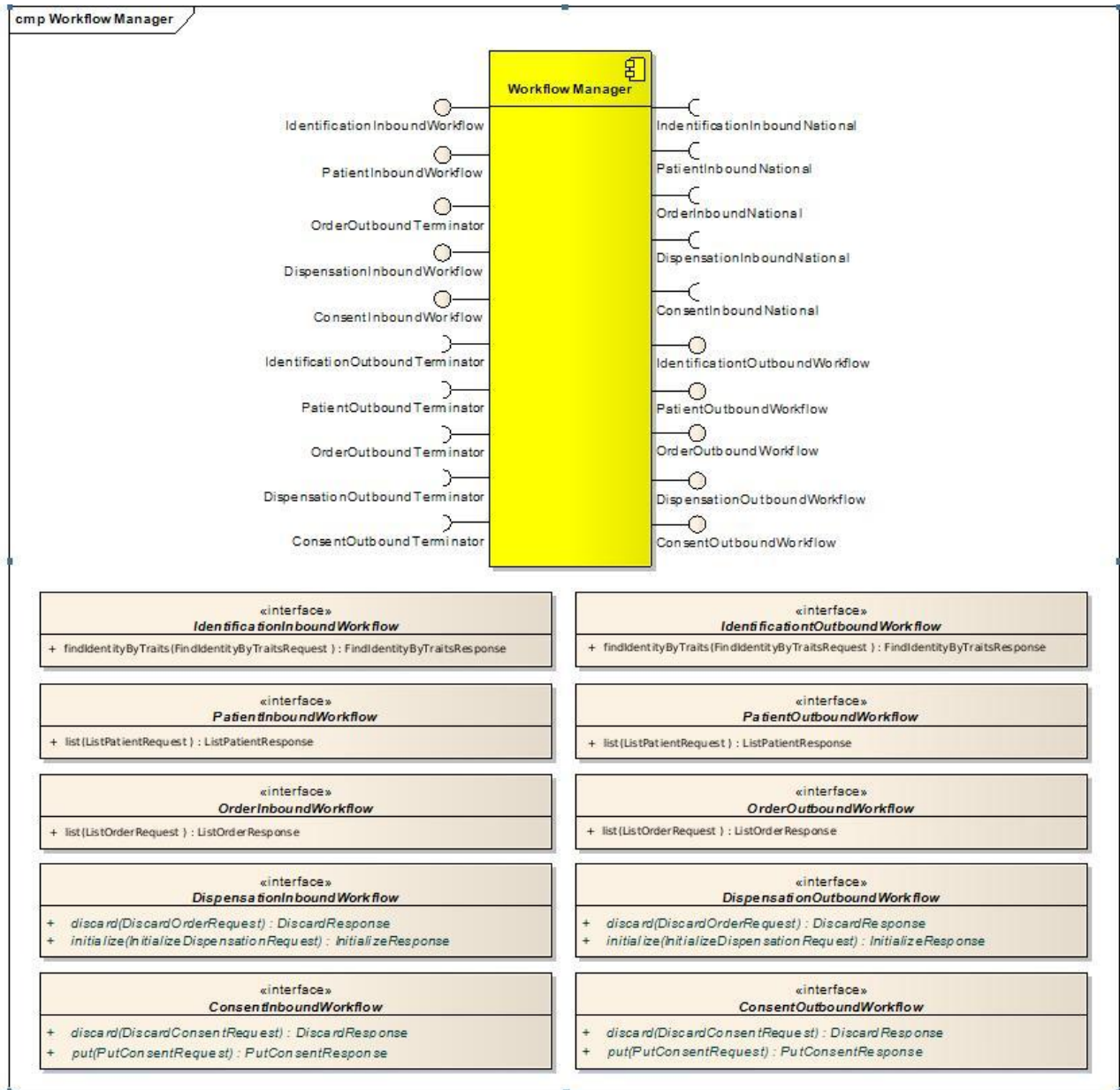



Figure 35: Workflow Manager


The WorkflowManager conducts the invocation of components to process requests. In software architecture this component isolates business logic from input and presentation to other Component. It eases independent development, testing and maintenance.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

The WorkflowManager runs the epSOS medical data (WP3.5) and add new logic for example, calculating if the patient has given his consent or not.

Different views can exist for the same data (e.g Patient Summary), and depends where the data is located (Business zone, NationalConnector zone, EpSOS zone), but the WorkflowManager receives the suitable data because the other components adapt the business model to the behavior of the WorkflowManager

The WorkflowManager that contain the business rules knows how to carry out specific tasks to other components.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

6.4.2.4 RoutingManager

This internal component is designed to implement the Routing objective.

This component provides interfaces for the EndPointDiscovery service acting as service point, in order to allow other components to know the service end point to be invoked to accomplish their tasks (e.g. patient identification).

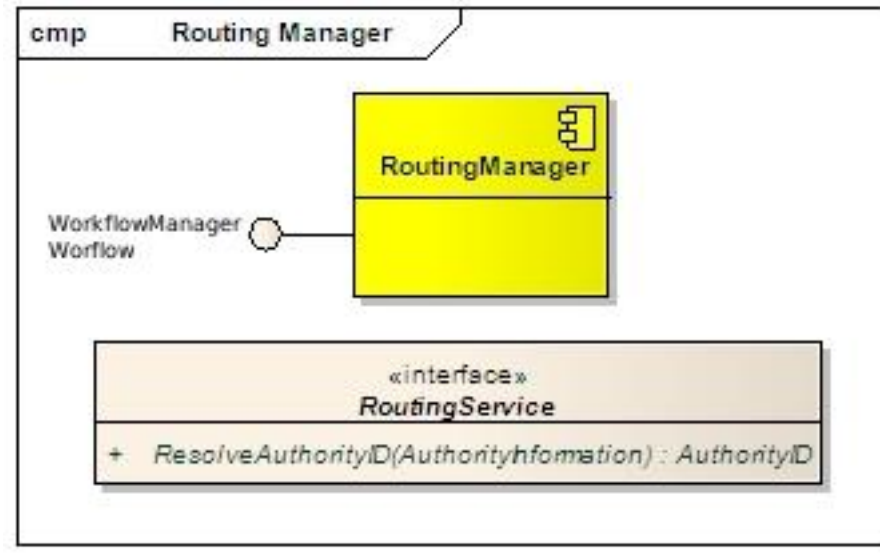



Figure 36: Routing Manager

Functions of the Routing Manager are implemented within an NCP by using a static configuration table. It is the responsibility of each NCP to keep the configuration up to date. It is the responsibility of each NCP to keep the configuration up to date. Please, refer to D3.4.2 for the format of the configuration files based on the ETSI TS 102 231 standard.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

6.4.2.5 Transformation Manager

The TransformationManager component is in charge of the following activities:

- Translating and/or transcoding (if necessary) the original data compliant to epSOS CDA syntax from the national language and possibly from the national code system(s) in the document creator country (in most cases Country A) to the epSOS Reference Terminology.
- Creating an epSOS unstructured CDA by embedding the original data from document creator presented in the pdf format. This data must be presented in a pdf format so that the document consumer country can read it.
- Translating the coded data elements from the epSOS Reference Terminology to the national language in document consumer country (in most cases Country B).

Note: That a relationship Must exists between the epSOS pivot document and the embedded PDF CDA

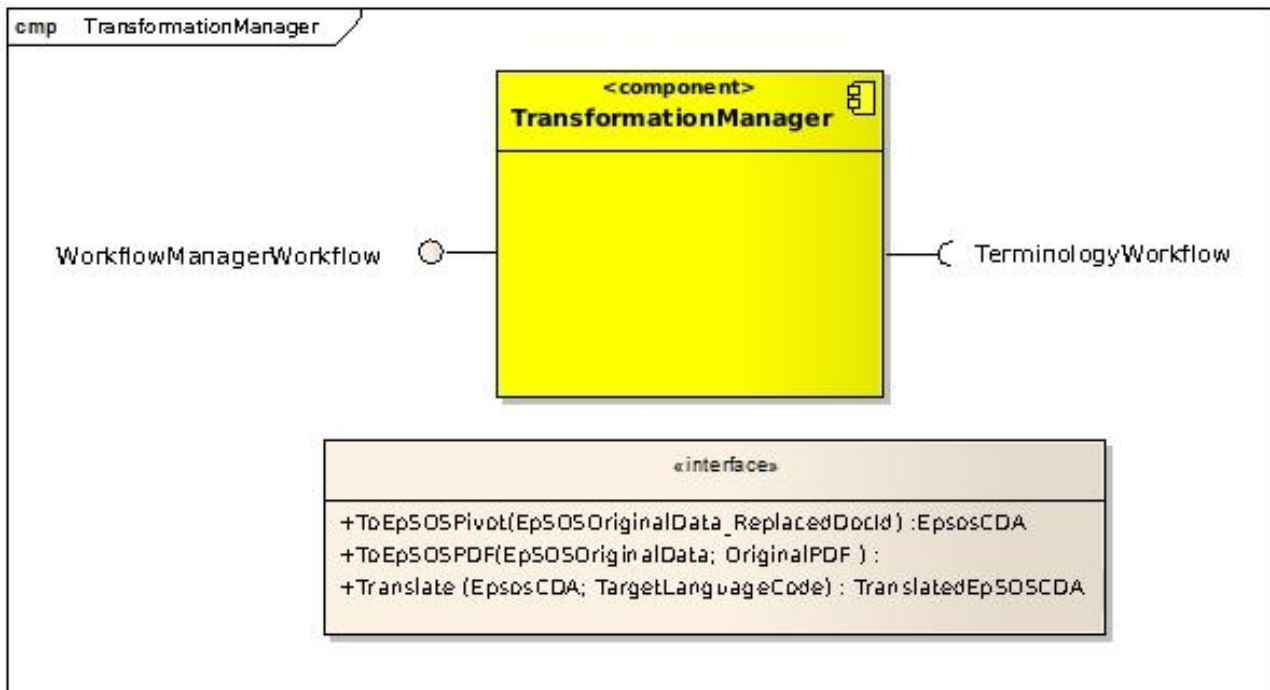


Figure 37: Transformation Manager



D3.3.2_v1.4	Document Short name: D3.3.2
	Version: 1.4
WP3.3: System architecture	Date: 30/04/2010

ToEpSOSPivot(EpSOSOriginalData_ReplacedDocId) :EpsosCDA

Textual description of operation	
<p>Transformation of national data to epSOS pivot format :</p> <p>After having received a <i>toEpSOSPivot()</i> request, this component takes the EpSOSOriginalData (already compliant to epSOS CDA syntax) and using the TAS capabilities, accomplishes the eventual transcoding of the terms present in the epSOS value sets, while also keeping the original codes and display name. An epSOS pivot document with epSOS coded concepts is therefore produced. The epSOS pivot document shall have a link to the EpSOSOriginalData.</p> <p><i>Exceptions:</i> in case of processing error or warning the responseStatusStructure should be properly valorized.</p>	
Input parameters	<p>EpSOSOriginalData : Medical document in its original data format as provided from the NationalConnector to this component. [Mandatory]</p> <p>ReplacedDocId is an instance identifier describing the document to be replaced.</p>
Output parameters	<p>EpSOS CDA structure</p> <p>Response structure including the epSOS pivot CDA and the response status structure.</p> <p>The response status structure provides information about the operation results, including possible errors and warning.</p>
Notes	



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture

Date: 30/04/2010

ToEpSOSPDF(EpSOSOriginalData; OriginalPDF) : EpSOSPDF

Textual description of operation

Transformation of national data to epSOS pivot format :

After having received the *ToEpSOSPDF()* request, this component takes the EpSOSOriginalData and the OriginalPDF and generates an unstructured CDA embedding the PDF using the information already present in the EpSOS original data. As a final result the PDF embedded CDA is returned to the requesting component. The embedded PDF CDA shall to have a link to the EpSOSOriginalData.

Exceptions: in case of processing error or warning the responseStatusStructure should be properly valorized.

Input parameters

EpSOSOriginalData

Medical document in its original data format as provided from the NationalConnector to this component. [Mandatory]

OriginalPDF

Printable representation (PDF/A) of the original national data as we expect have been seen by the originator HCP [Mandatory].

Output parameters

EpSOSPDF structure

response structure including the epSOS unstructured CDA embedding the original pdf and the response status structure.

The response status structure provides information about the operation results, including possible errors and warning.


Notes



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

Translate (EpsosCDA; TargetLanguageCode) : TranslatedEpSOSCDA

Textual description of operation	
<p>Translation from epSOS pivot data to consumer country language :</p> <p>After having received a <i>translate()</i> request, this component starts to process the received <i>EpSOSosCDA</i> in order extract the epSOS coded concepts.</p> <p>Subsequently, for each coded concept found, it makes use of the TSAM capabilities for the purpose of obtaining the representation of that concept in the target <i>TargetLanguageCode</i> identifier . This information is therefore used by this component to update the <i>displayName</i> attribute of that coded entry.</p> <p>After the completion of this translation phase, an epSOS pivot document with “translated” concepts is obtained.</p> <p>This document is therefore returned to the requesting party. No changes are applied to the document identifiers.</p> <p><i>Exceptions:</i> in case of processing error or warning the <i>responseStatusStructure</i> should be properly valorized.</p>	
Input parameters	<p>EpSOSosCDA Document in epSOS pivot format (with epSOS codes)</p> <p>TargetLanguageCode. Identifier (code) of the target language.</p>
Output parameters	<p>TranslatedEpSOSCDA epSOS pivot CDA with translated epSOS codes into the consumer country language.</p>
Notes	

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

6.4.2.6 Terminology Access Manager

Terminology Access Manager has two roles :

- Translating a given concept designation into the requested target language using the information present in the Terminology Repository. translation stands for the capability of associating to an epSOS coded concept the localized concept description or display name: i.e. the translation into the target language of the “concept” conveyed (e.g. code “30001000” EDQM can have the display names “Φύσιγγα”, “Ampulka” or “Ampoule”, depending on where it is used.)
- Transcoding a given “local” coded concept into the appropriate epSOS coded concept using the information present in the Terminology Repository. Transcoding means the capability of getting the epSOS quasi-synonymous²⁷ associated to a “local” coded concept.

²⁷ i.e. a coded concept derived from the appropriate epSOS Value Set semantically equivalent to a given coded concept.

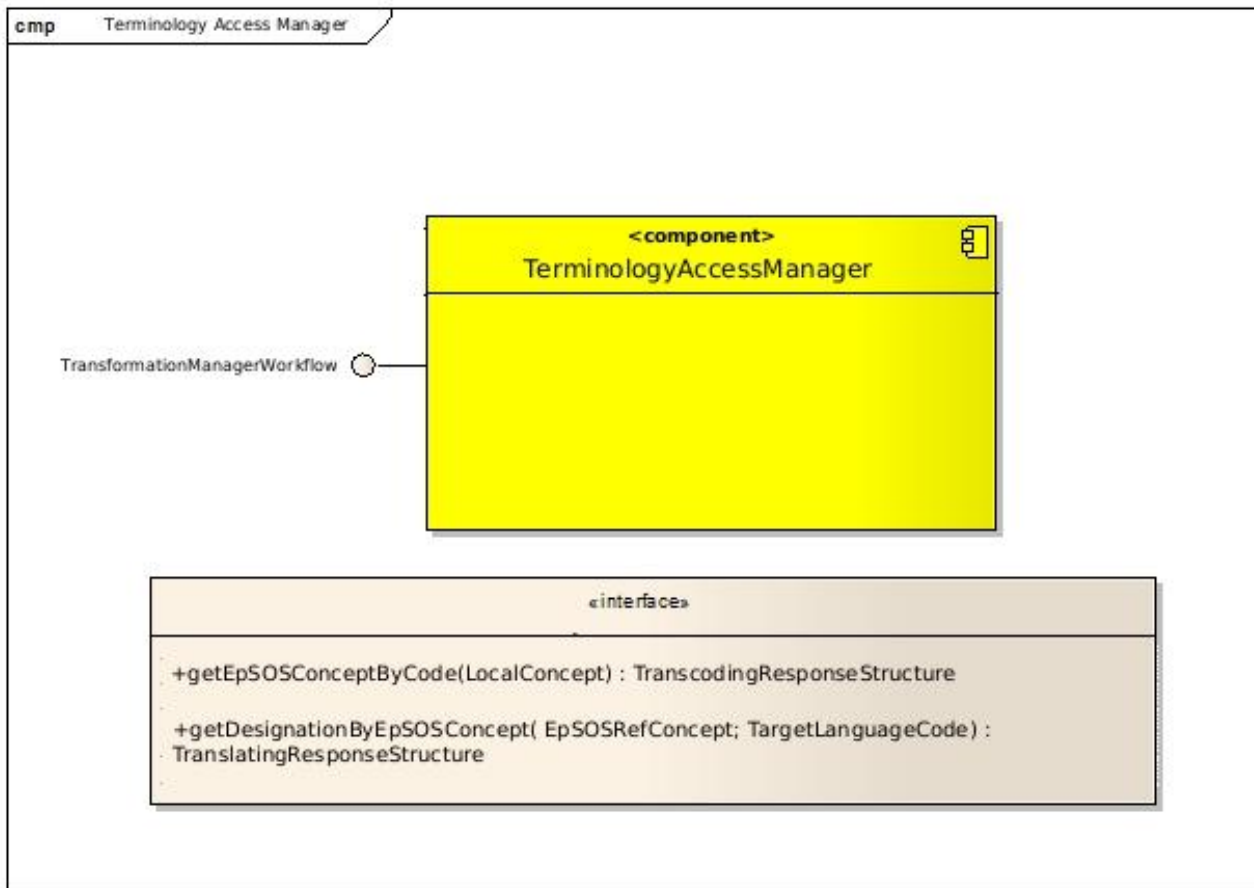


Figure 38: Terminology Access Manager

The epSOS Reference Terminology has as a starting point the epSOS MVC (Master Value Sets), which in turn is the basis for the epSOS MTC (Master Transcoding Catalogue see 3.5.2 for further details). The mapping activity from the “local” coded concept to the epSOS Value Sets present in the epSOS MVC is out of scope of epSOS and it is the responsibility of the National Linguistic Competence Centers from each Member State.



D3.3.2_v1.4	Document Short name: D3.3.2
	Version: 1.4
WP3.3: System architecture	Date: 30/04/2010

getEpSOSConceptByCode(LocalConcept) : TranscodingResponseStructure

Textual description of operation	
<p>Transcoding a given “local” coded concept into the appropriate epSOS coded concept using the information present in the Terminology Repository.</p> <p>This component issues an getEpSOSConceptByCode_() request in order to know the best matching epSOS Concept, according to the information provided.</p>	
Input parameters	<p>LocalConcept;</p> <p>the LocalConcept structure in order to search within the Terminology Repository for the best matching epSOS Concept, according to the local information provided (e.g., if no code system version is indicated, the latest version will be provided).</p>
Output parameters	<p>TranscodingResponseStructure</p> <p>Response structure including:</p> <ol style="list-style-type: none"> 1. the epSOS Reference Concept: this means the Concept Code, the English designation, the concept code system (OID), Code System Version, Value Set OID; Value Set Version, 2. The responseStatusStructure, providing information about operation result, including possible errors and warning.
Exceptions	<p>in case of not existing transcoding or processing error the responseStatusStructure should be properly valorised</p>



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture

Date: 30/04/2010

**getDesignationByEpSOSConcept(EpSOSRefConcept; TargetLanguageCode)
: TranslatingResponseStructure**

Textual description of operation	
<p>Translating a given concept designation into the requested target language using the information present in the Terminology Repository :</p> <p>This component issues getDesignationByEpSOSConcept_() request in order to know the target language epSOS Designation, according to the information provided.</p>	
input parameters	<p>EpSOSRefConcept.</p> <p>EpSOSRefConcept structure in order to search within the Terminology Repository for the target language epSOS Designation, according to the local information provided</p>
Output parameters	<p>translatingResponseStructure</p> <p>Response structure including:</p> <ol style="list-style-type: none"> 1. the target language concept designation; 2. the responseStatusStructure providing information about operation result, including possible errors and warning.
Exceptions	<p>in case of not existing translation or processing error the responseStatusStructure should be properly valorised</p>

6.4.2.6.1 *Interaction diagrams for semantic*

This section describes the two interaction uses in which the Semantic Components are involved:

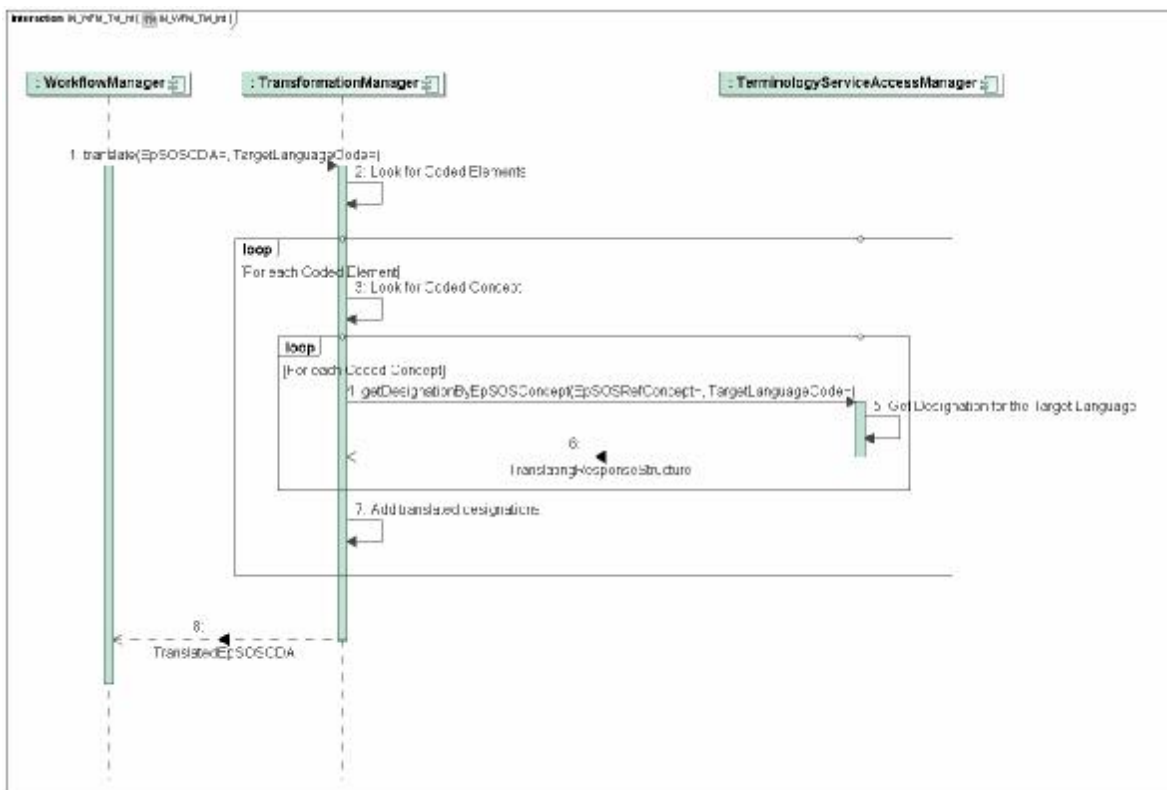


Figure 39: EpSOS CDA traduction

This interaction is used for the purpose of obtaining the epSOS pivot CDA and the CDA with the original PDF embedded. It shows the WorkflowManager to ask for the translation of the epSOS CDA document.

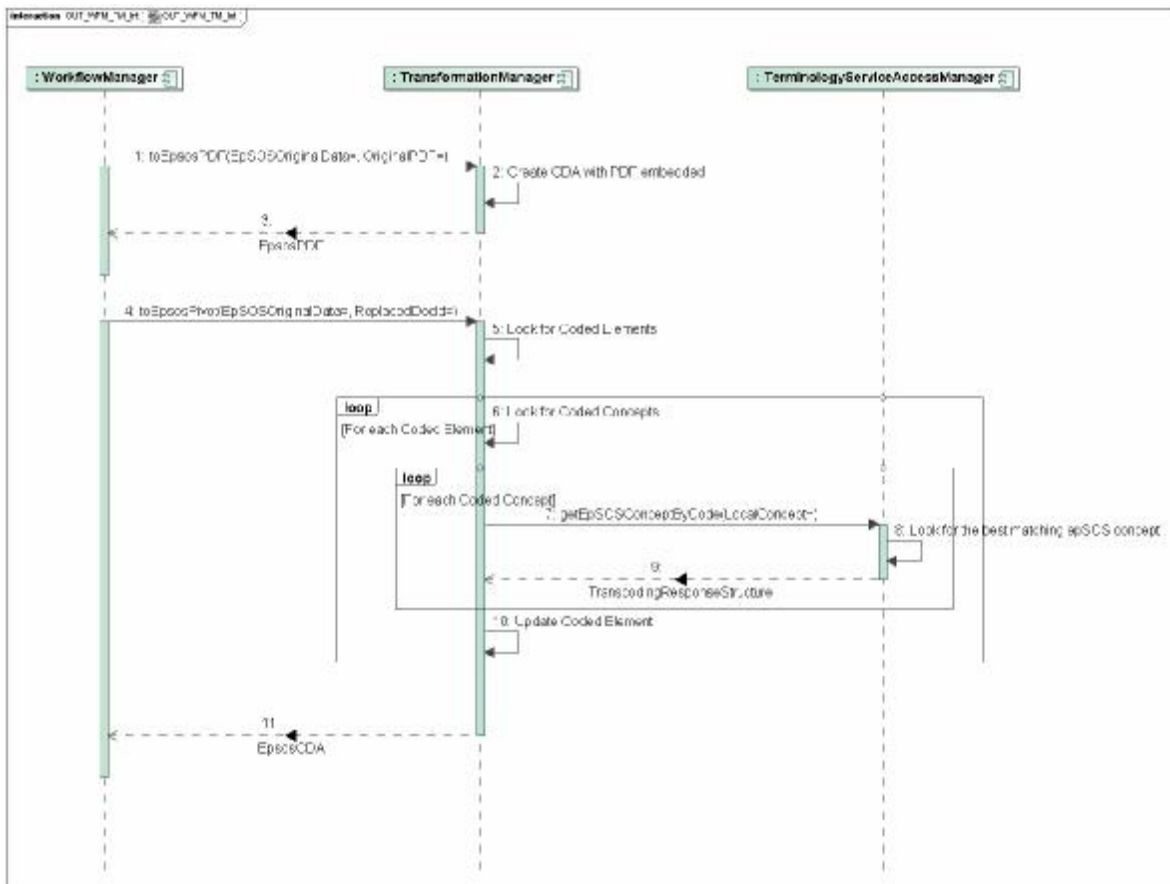



Figure 40: Transformation to epSOS CDA

This interaction is used for the purpose of obtaining a translated version of the epSOS pivot CDA into the target language.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

6.4.2.7 Security Manager

The SecurityManager component is responsible for creation and verification of digital signatures that are applied to medical documents.

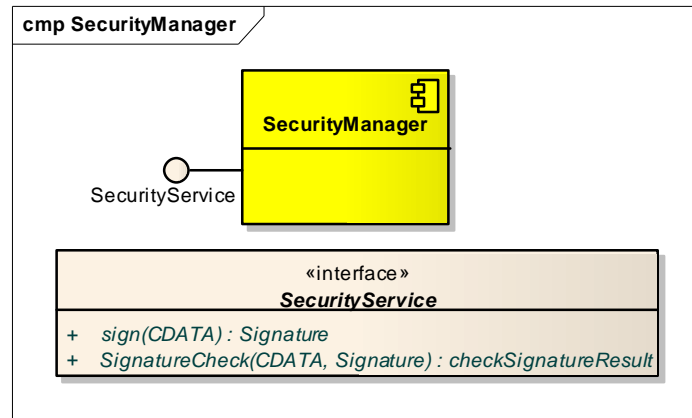


Figure 41: Security Manager

sign(CDATA) : Signature


Textual description of operation	
<p>This operation processes a XML DSig signature for a given XML according to the XML DSig standard and the epSOS specifications.</p> <p>Only known documents are signed and before the signature processing a schema validation is done. The documents that are known are configurable.</p>	
Input parameters	CDATA XML Document to sign
Output parameters	SignedDocument



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

CheckSignature(CDATA, Signature) : CheckSignatureResult

Textual description of operation	
The XML DSig signature of a XML document is validated including the validation of the certificate that confirmed the signature.	
Input parameters	CDATA XML containing Signature Digital signature
Output parameters	CheckSignatureResult Encoded in the status information are <ul style="list-style-type: none"> • Validity of signature • Validity of certificate
Notes	All the known and trusted certificates have to be registered by configuration beforehand.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

6.4.2.8 AuditTrail

This internal component is designed to implement the Audit Trail objectives.

This component provides interfaces for the Audit Trail Service acting as service point, in order to keep track of events to be logged.

This AuditTrail component is responsible for receiving an EventLog message in an ATNA-compatible way

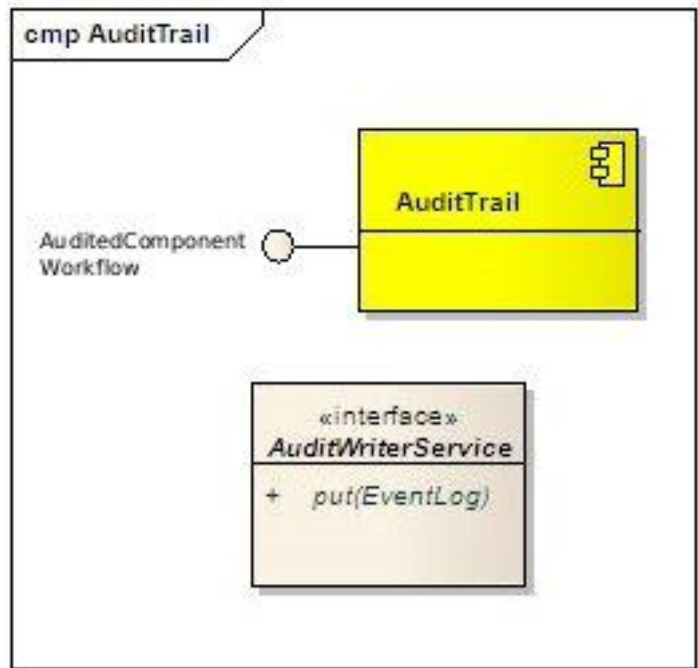



Figure 42 Audit Component

put (EventLog)

The AuditTrail accept an audit trail entries in an ATNA-compatible way, encapsulated in the Event Log. This document does not give detail for the storage procedure of the audit records. See WP 3.8 for further details. The Audit Trail function is considered to be sufficient for data non repudiation and traceability, if a failure occurs.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

6.4.2.9 Routing Manager

NCP endpoint addresses lookup. The address lookup table is a XML-document that can be stored in the NCP's local file system or be fetched (and cached) from a URL of a central service.

Note : there is an open issue pending : does the Routing Manager fecht an OID and a URL (TCONF 2010/04/08)

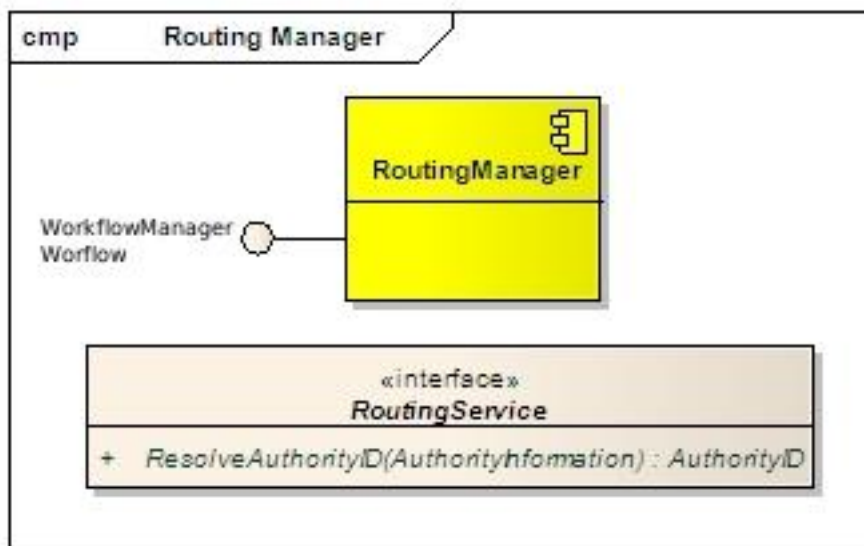



Figure 43: Routing Manager

ResolveAuthorityID(AuthorityInformation) : AuthorityID

Textual description of operation	
The result of this operation is the OID of the inbound gateway that has to be requested. It is not specified yet in which ways this OID can be resolved. Therefore the input parameters are not stable.	
Input parameters	AuthorityInformation Not specified in which way authority information is coded.
Output parameters	AuthorityID OID which clearly references the inbound gateway that will be requested.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

6.4.2.10 Configuration And Monitoring Manager

This subcomponent should be responsible for analyzing the audit trail and, based on a configurable way easy to maintain for administrator. Alert should prevent possible abuses (such as excessive requests issued from a HCP or a patient is queried from more than one country at a time).

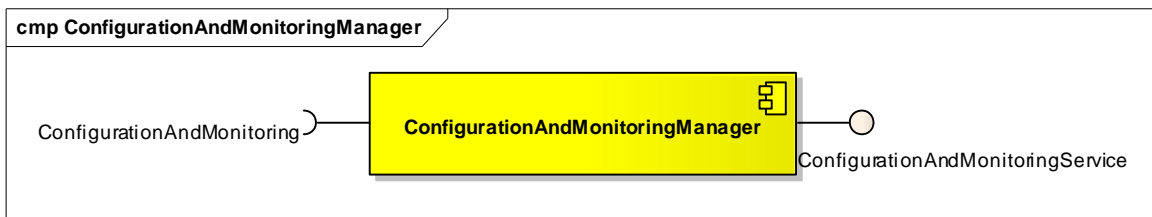


Figure 44: Configuration and Monitoring

Configuration and Monitoring Manager is responsible for keeping epSOS configuration, at the application boot start, the synchronicity with central epSOS repository (e.g. NCP routing and taxonomy access). Process for Synchronicity establishment is not sketch in this document.

The monitoring can detect fraud, according WP 3.7 requirement.

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

6.4.2.11 NationalConnector

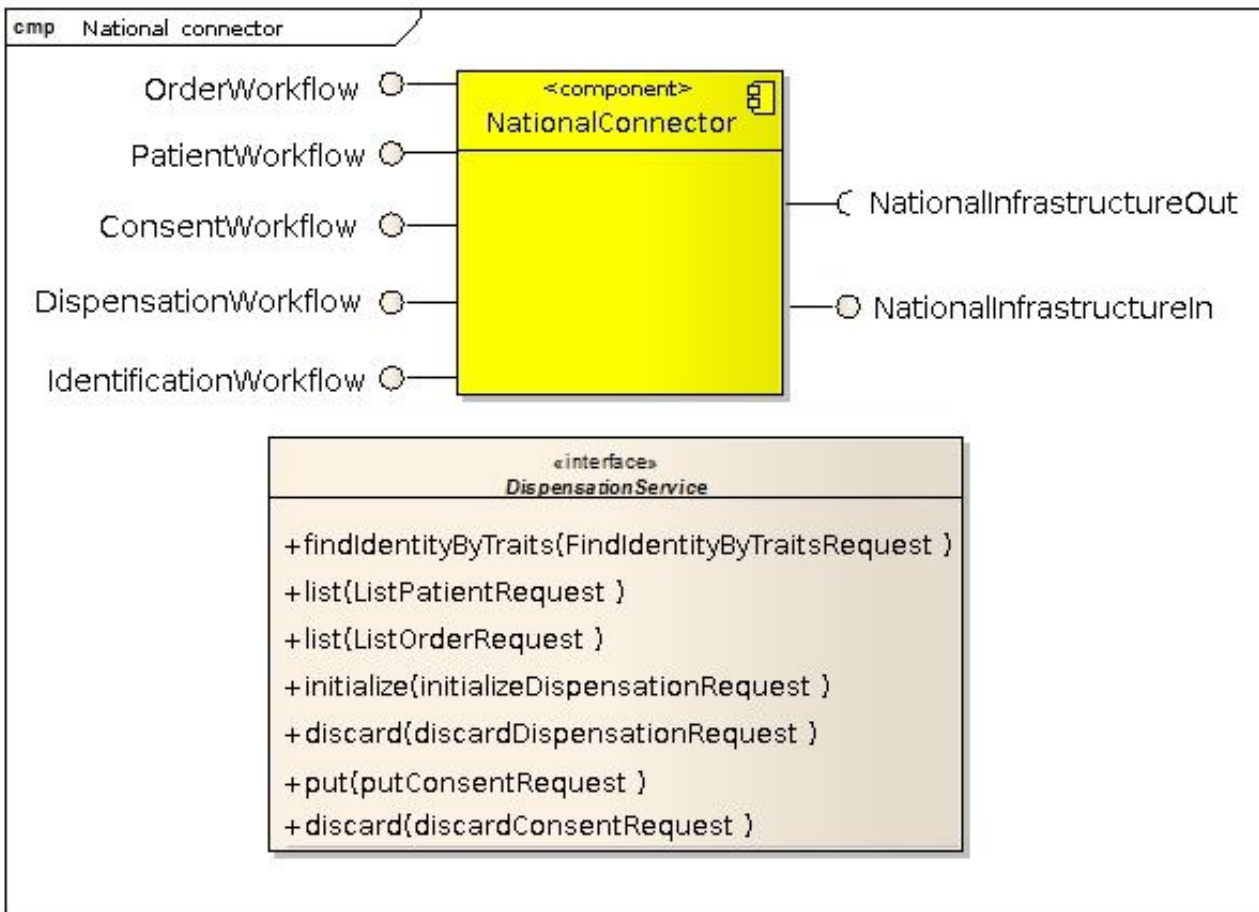



Figure 45 National Connector

This component is designed to implement the objectives related to National Infrastructures connection and National Data handling, only the interfaces can be common between MS. The implementation is a very specific task for each MS, and depends and the national infrastructure.

To draw a parallel, **National Connector is like a plug or a socket** as devices for removably connecting the NCP. MS must design the socket to be able to plug to the National Connector. Because plugs over countries can be different, implementation of the National Connector is different.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

The National Connector maps logical functional Components of the NCP to the national Infrastructure. D3.3.2 does not provide specific implementation guidelines.

MS MUST provide storage and be able to handle the medical Data persistence (PS, eP, Consent). The NationalConnector is the entry and exit point from and to the NCP. MS are free to develop and build the implementation of the National Connector with the interfaces define in this document. MS can export the interface as service, to communicate with the NationalConnector needed.

6.4.3 Components Communication workflow

6.4.3.1 Patient Identification

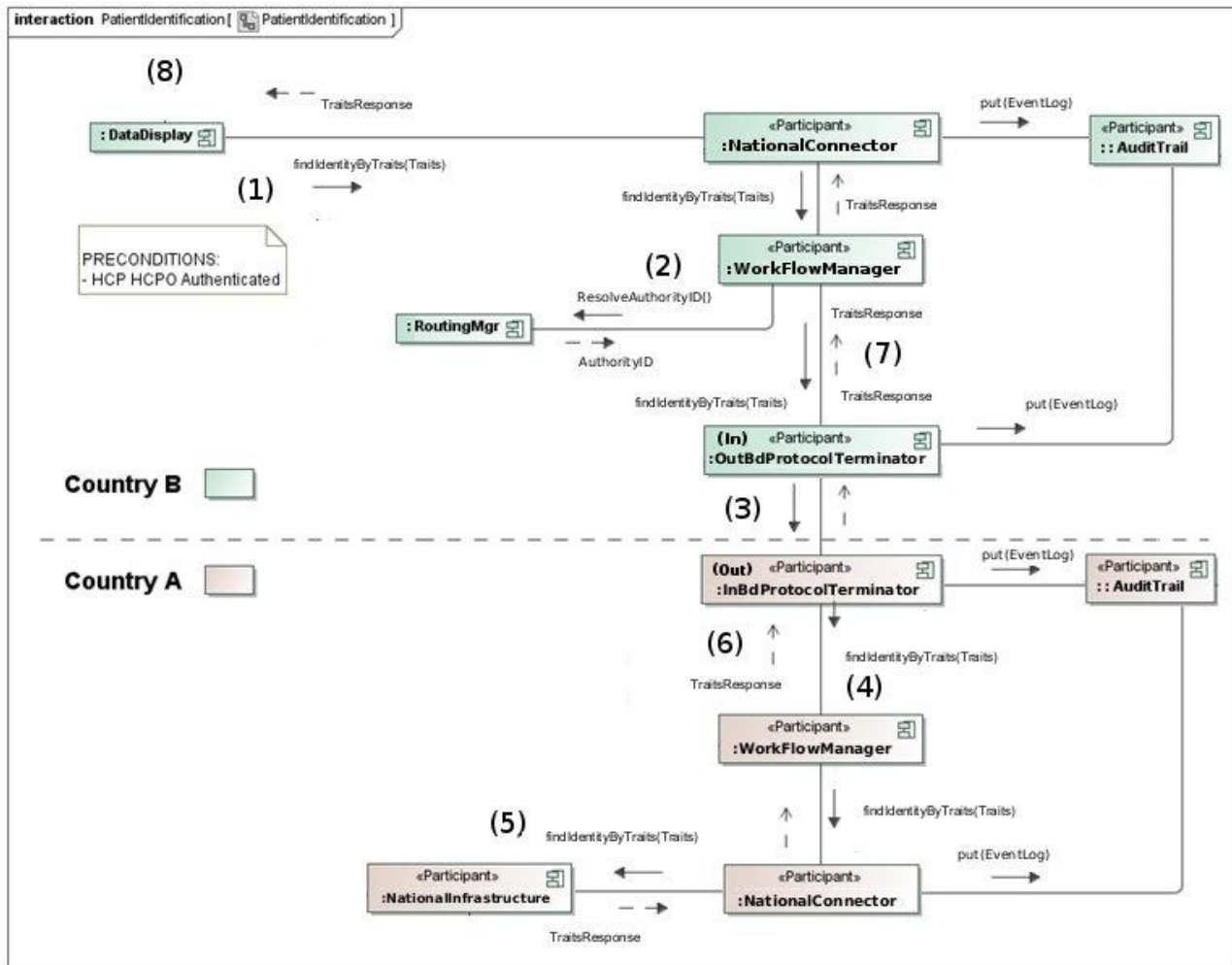


Figure 46: PatientIdentification

1. After the HCP(O) B is authenticated (precondition), the component dataDisplay initiates the searchPatient, by calling the right function located on the NationalConnector. The findIdentityByTraits() needs patient attributes as input arguments (The name of the transaction : findIdentityByTraits() is not mandatory, it is MS decision.) . All incoming transactions at the NationalConnector are audited by the AuditTrails component.

2. The request is forward to the WorkflowManager, where the business logic starts. The RoutingManager informs the WorkFlowManager for the NCP A destination.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

3. The NCP B OutboundProtocolTerminator wraps the request into a SOAP envelope and send it to the InboundProtocolTerminator in A. Audit Trails B keeps track of what does leave from country B, as the same occurs in country A when the message arrives. Any incoming message that arrives to the InboundProtocolTerminator for the request contains the wrapped informations for the patient. Decoding and unwrapping is done inside in the InboundProtocolTerminator.

4. The WorkflowManager extracts the identity traits from the object and uses them as an input arguments when calling *NationalController for the findIdentityByTraits() operation*.

5. The NationalConnector queries the patient Data result in from the national infrastructure in A and the returns the object to the Workflow Manager. The transaction is audited by the AuditTrails component. The name of the transaction : findIdentityByTraits() is not mandatory, it is MS decision.

6. The Traits Patient Response goes back to NCP B through the same components (1-5), and arrives to the Inbound Terminator in B (previously named OutBoundTerminator when message goes out). Upon the arrival of the SOAP response, both ProtocolTerminator makes a corresponding record in the audit trail.

7. The WorkFlowManager in B receives the unwrapped message from InboundProtocolTerminator and transmit the request to the NationalConnector in B.

8. The Patient Identification Response Traits is returned to the originator of the request, the HCP B.

6.4.3.2 *Data Exchange (PS & EP)*

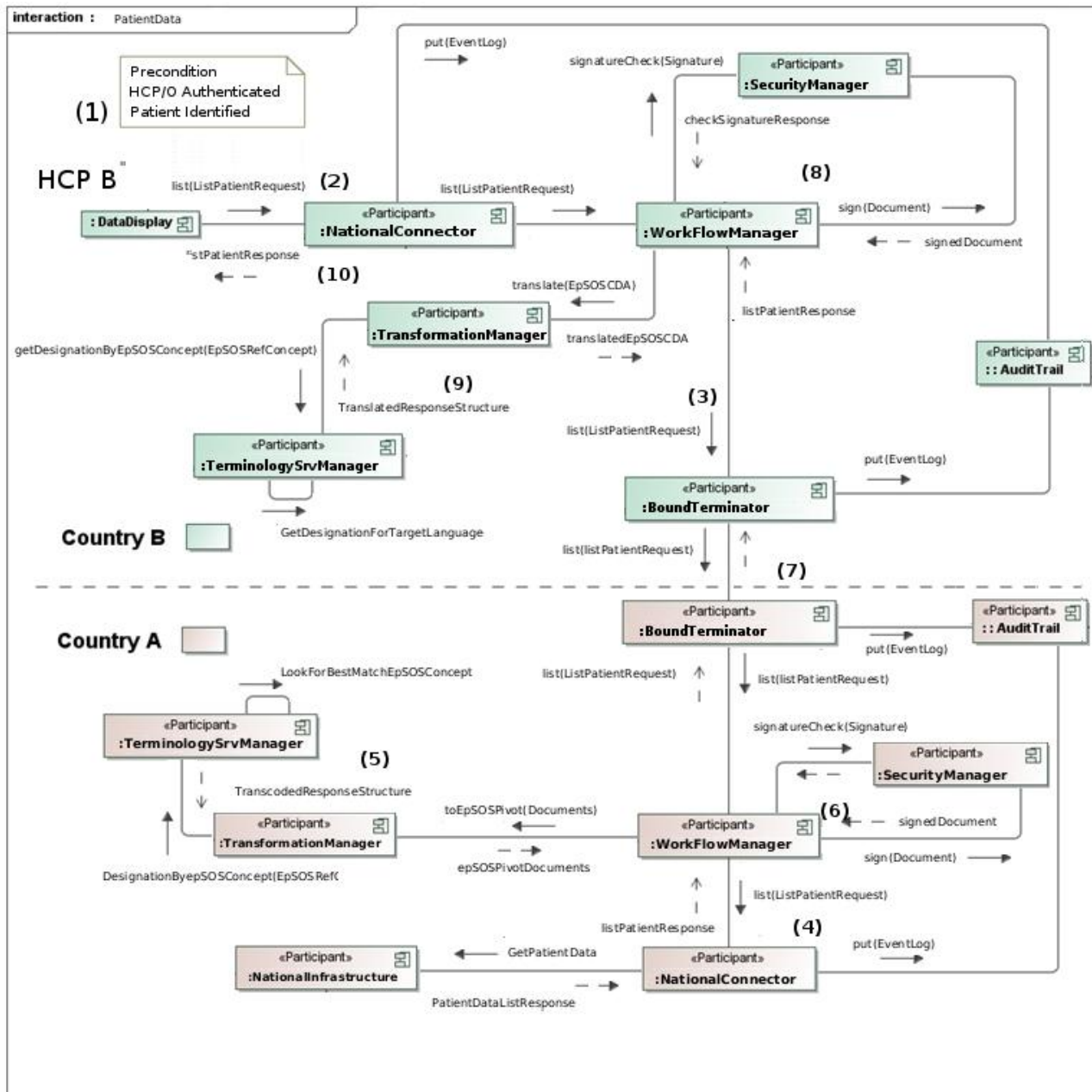



Figure 47: Patient data workflow

1. HCP/O B is authenticated and the patient is identified (Precondition). The HCP calls for retrieving prescriptions of the patient by calling a corresponding method located at the *NationalConnector* in B and providing ID of the patient. The call list (the wording :

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

“ListPatientRequest” is not mandatory) is initiated by the HCP B data display component (HCP B Portal see JWP WP3.8).

2. The *AuditTrail* component keeps track of the message passing through the *NationalConnector*. (The same audit is done when the response returns). The *AuditTrail* is considered to be sufficient for data non repudiation, if a failure occurs. The *NationalConnector* forwards the request to *WorkflowManager*.

3. The *WorkflowManager* forwards the request to *OutboundProtocolTerminator* (named *BoundTerminator* on the figure, because the name switches between *In* and *Out*). The *SecurityManager* function *Sign()* the message with the NCP-B signature.


4. After the message passed through the terminators and arrives at the *WorkFlowManager* in A. The *NationalConnector* make the appropriate call to the national infrastructure and records the request in the audit trail. The response should contain requested prescriptions in the national format of MS A. On the figure, the *GetPatientData* action and response is a MS transaction.

5. The *WorkflowManager* receives the response from *NationalConnector* and calls The *TransformationManager* to obtain the epSOS pivot CDA and the CDA with the original PDF embedded.

6. The *WorkflowManager* calls the *SecurityManager* component, and sign the XML Message with the NCP- A signature

7. The NCP A *OutboundProtocolTerminator* wraps the request into a SOAP envelope and send it to the *InboundProtocolTerminator* in B (*BoundTerminator*). *Audit Trails* keeps track of messages exchanged. The incoming message that arrives in B contains the wrapped informations for the patient.

8. *WorkflowManager* transfers patient data to *SecurityManager* for the signature verification.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

9. For the purpose of obtaining a translated version of the epSOS pivot CDA into the B country language, the WorkflowManager get the return data from the TransformationManager.

10. Patient data is returned to the HCP B, if the message has passed successfully all the steps.

The proposed interfaces might support other retrieval mechanisms too, as retrieving documents by setID. For the scope of this project, considering that only one Patient Summary may exist and a limited number of prescriptions are usually active, it's reasonable to suppose the usage of a "direct" request for retrieval through the list() operation. The treatment relationship (as a SAML assertion signed by NCP B or HCP) is covered in the security chapter.

6.4.3.3 *Notification*

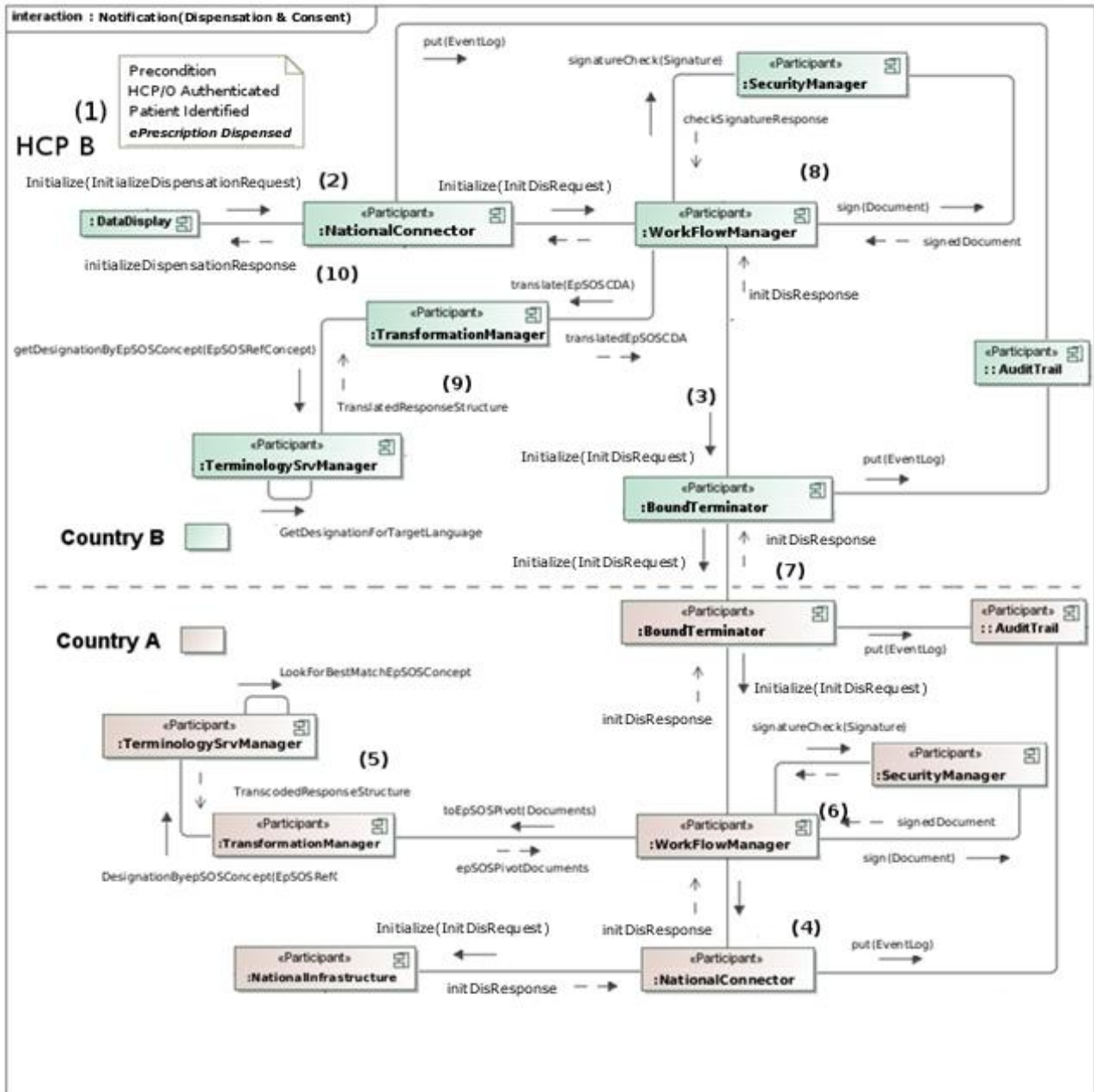



Figure 48: Notification Workflow

1. HCP/O B is authenticated and the patient is identified (Precondition). The HCP calls for retrieving prescriptions of the patient by calling a corresponding method located at the *NationalConnector* in B and providing ID of the patient. EPrescription has been already

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

delivered to the pharmacy. The call initialize (InitializeDispensationRequest) is initiated by HCP B data display component (HCP B Portal see JWP WP3.8).

2. The *AuditTrail component* keeps track of the message passing through the *NationalConnector*. (The same audit is done when the response returns). The *NationalConnector* forwards the request to *WorkflowManager*.

3. The *WorkflowManager* forwards the request to *OutboundProtocolTerminator* (named *BoundTerminator* on the figure, because the name switches between *In* and *Out*). The *SecurityManager Sign()* the message with the NCP-B signature.

4. After the message passed through the terminators and arrives at the *WorkFlowManager* in A. The *NationalConnector* make the appropriate call to the national infrastructure and records the request in the audit trail. The response should contain requested prescriptions in the national format of MS A.

5. The *WorkflowManager* receives the response from *NationalConnector* and calls The *TransformationManager* to obtain the epSOS pivot CDA and the CDA with the original PDF embedded.

6. The *WorkflowManager* calls the *SecurityManager* component, and sign the XML Message with the NCP- A signature

7. The NCP A *OutboundProtocolTerminator* wraps the request into a SOAP envelope and send it to the *InboundProtocolTerminator* in B (*BoundTerminator* in the figure). *Audit Trails* keeps track of messages exchanged. The incoming message that arrives in B contains the wrapped informations for the patient.


8. *WorkflowManager* transfers patient data to *SecurityManager* for the signature verification.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010
WP3.3: System architecture		

9. For the purpose of obtaining a translated version of the epSOS pivot CDA into the B country language, the WorkflowManager gets the return data from the TransformationManager.

10. Patient datas is returned to the HCP B, if the message has passed successfully all the steps.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

6.5 Interfaces

6.5.1 *epSOS Gateway Interfaces*

Service	Mediated Data
Patient Identification Service	Patient ID traits
Patient Service	Patient summary documents
Order Service	ePrescription documents
eDispensation Service	eDispensation documents
Consent Service	Consent documents

6.5.1.1 *IdentificationService*

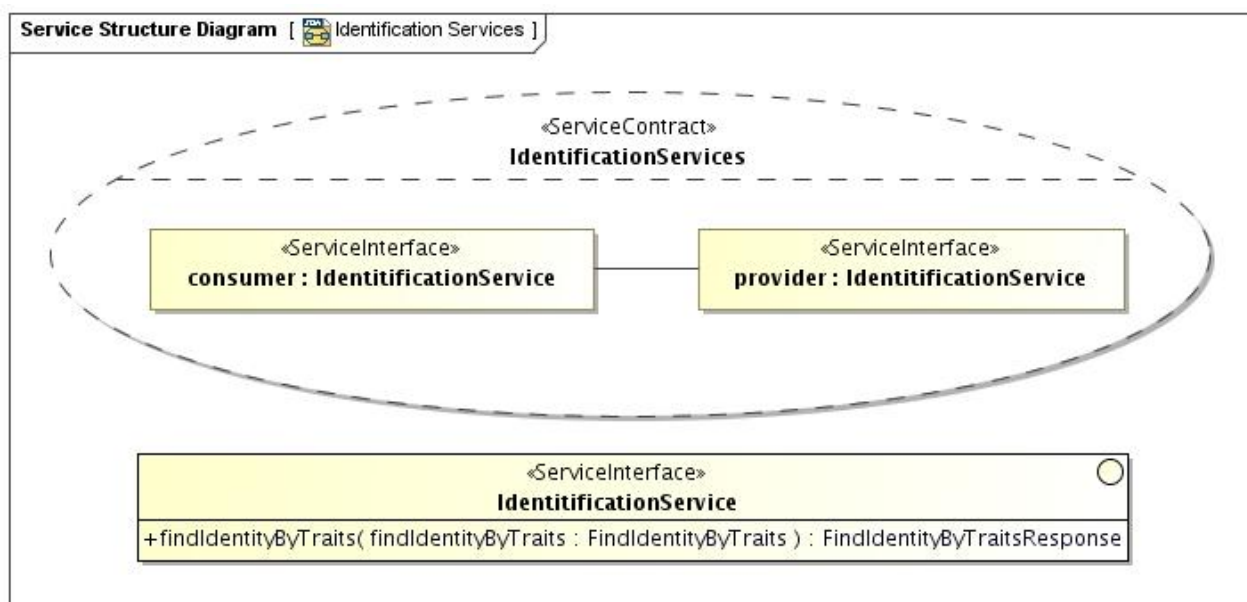


Figure 49: Identification Service

NCP interacts with other NCPs through this service in order to request patient identification traits for her/his identification. The Consumer/Requestor operate from MS B. In order to discover a patient's data the patient must be identified with a unique patient identifier. A shared identifier let properly reference patients data which is provided by the medical data service at the patient's country of affiliation. This shared identifier MUST be



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

used as a patient identifier required for the epSOS medical data exchange services (e. g. patient service and order service).

Operation	<code>findIdentityByTraits()</code>				
Description	Obtain a shared patient identifier by querying for patient identity traits				
Requestor	Consuming Gateway at NCP-B				
Input Message	FindIdentityByTraitsRequest				
	<table border="0"> <tr> <td style="padding-right: 20px;">Body</td> <td>(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.</td> </tr> <tr> <td>Security Token</td> <td>X.509 Gateway Certificate epSOS HCP Identity Assertion</td> </tr> </table>	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	X.509 Gateway Certificate epSOS HCP Identity Assertion
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	X.509 Gateway Certificate epSOS HCP Identity Assertion				
Output Message in successful Case	FindIdentityByTraitsResponse				
	<table border="0"> <tr> <td style="padding-right: 20px;">Body</td> <td>(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.</td> </tr> <tr> <td>Security Token</td> <td>X.509 Gateway Certificate</td> </tr> </table>	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.	Security Token	X.509 Gateway Certificate
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.				
Security Token	X.509 Gateway Certificate				
Precondition of success scenario	<ol style="list-style-type: none"> 1. The requestor is able to locate the service provider 2. The certificate of the NCP-A gateway is available to the requestor. 3. The requestor is able to verify the certificate of the NCP-A gateway. 4. The NCP-A gateway is able to verify the requestor's certificate. 5. An HCP identity assertion has been issued by NCP-B and is available to the requestor 6. The NCP-A gateway is able to verify the validity of the HCP identity assertion 				
Main success scenario	Actions of the epSOS Patient Identification Service provider: <ol style="list-style-type: none"> 1. validate the message signature and decrypt the message body 2. verify HCP identity assertion 3. extract the patient identity traits from the message body 4. search for patients that match the provided ID attributes 5. discard all patients from the candidates list who have not given consent to epSOS 6. if no patient matches: throw respective fault 7. if multiple patients match: request for more identity traits 8. if single patient matches: select ID to be used for subsequent requests 9. sign the response message and send it to the requestor 				
Fault Conditions	Preconditions for a success scenario are not given Requestor has insufficient rights to query for a patient's identity No matching patient is discovered that gave consent to epSOS ID traits are insufficient to find a unique match The confidence level of the matches is too low with respect to the level required by the requestor.				

6.5.1.2 *PatientService (Patient Summary)*

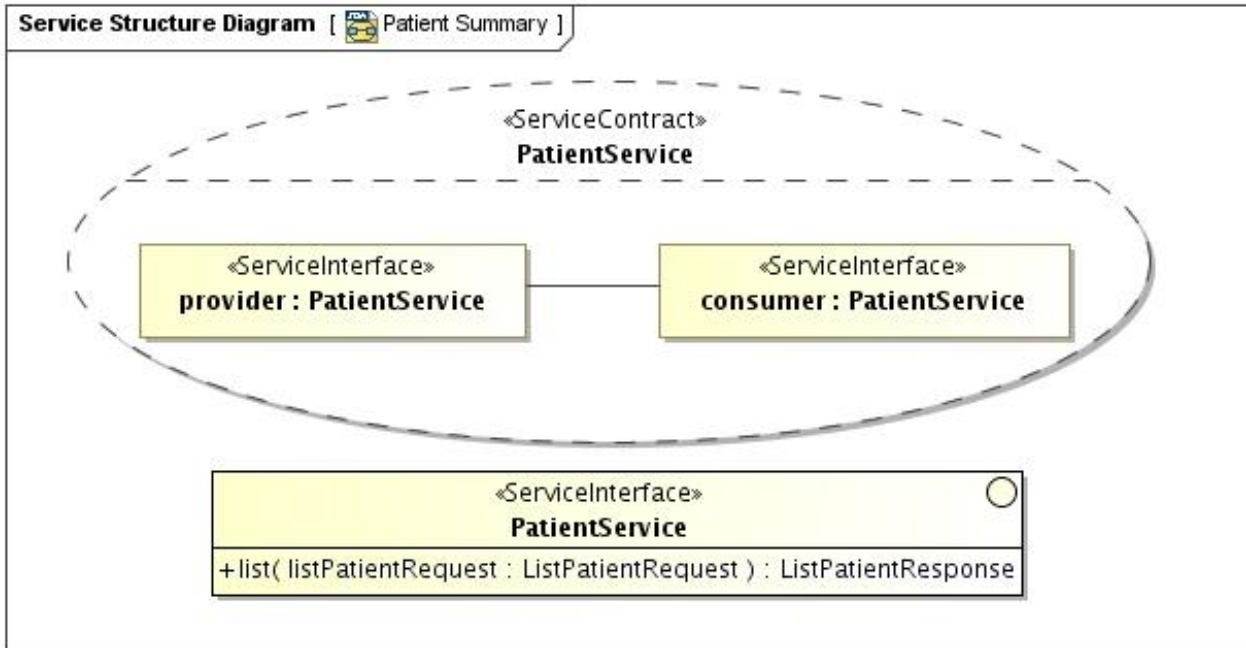


Figure 50: Patient Service

This service is used to obtain the patient summary documents response.

Operation	<code>list()</code>				
Description	Obtain the patient summary of the identified patient				
Requestor	Consuming Gateway at NCP-B				
Input Message	ListPatientRequest				
	<table border="1"> <tr> <td>Body</td> <td>Identifier of the patient whose patient summary is requested Optional: epSOS CDA template qualifier (pivot and/or source coded document)</td> </tr> <tr> <td>Security Token</td> <td>X.509 Gateway Certificate epSOS HCP Identity Assertion epSOS Treatment Relationship Confirmation Assertion (opt.)</td> </tr> </table>	Body	Identifier of the patient whose patient summary is requested Optional: epSOS CDA template qualifier (pivot and/or source coded document)	Security Token	X.509 Gateway Certificate epSOS HCP Identity Assertion epSOS Treatment Relationship Confirmation Assertion (opt.)
Body	Identifier of the patient whose patient summary is requested Optional: epSOS CDA template qualifier (pivot and/or source coded document)				
Security Token	X.509 Gateway Certificate epSOS HCP Identity Assertion epSOS Treatment Relationship Confirmation Assertion (opt.)				
Output Message in successful Case	ListPatientResponse				
	<table border="1"> <tr> <td>Body</td> <td>epSOS-encoded patient summary (CDA) or/and source coded patient summary (PDF) of the identified patient</td> </tr> </table>	Body	epSOS-encoded patient summary (CDA) or/and source coded patient summary (PDF) of the identified patient		
Body	epSOS-encoded patient summary (CDA) or/and source coded patient summary (PDF) of the identified patient				



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010
WP3.3: System architecture		

Security Token	X.509 Gateway Certificate
Precondition of success scenario	<ol style="list-style-type: none"> 1. The requestor is able to locate the service provider 2. The certificate of the NCP-A gateway is available to the requestor. 3. The requestor is able to verify the certificate of the NCP-A gateway. 4. The NCP-A gateway is able to verify the requestor's certificate. 5. An HCP identity assertion has been issued by NCP-A and is available to the requestor 6. The NCP-A gateway is able to verify the validity of the HCP identity assertion 7. NCP-A and NCP-B agreed on a common ID for referencing to the patient 8. An TRC assertion has been issued by NCP-B and is available to the requestor 9. The NCP-A gateway is able to verify the validity of the TRC assertion
Main success scenario	<p>Actions of the epSOS Patient Service provider:</p> <ol style="list-style-type: none"> 1. validate the message signature 2. verify HCP identity assertion and TRC assertion 3. extract the patient ID from the message body 4. verify that the patient has given consent to epSOS and that the consent is valid 5. retrieve patient's patient summary source document 6. enforce national security policy and (if available) patient privacy policy 7. verify authenticity and integrity of the patient summary 8. transform patient summary into epSOS pivot format (if requested and needed) 9. render PDF from source document (if requested and needed) 10. sign the response message and send it to the requestor
Fault	<p>Preconditions for a success scenario are not given</p> <hr/> <p>Requestor has insufficient rights to access the patient's medical summary</p> <hr/> <p>No patient summary is available for the identified patient</p> <hr/> <p>The patient summary cannot be provided in the requested encoding</p> <hr/> <p>Temporary failure (e. g. authenticity verification cannot be performed due to a PKI failure)</p>
Warning	<p>Country A allows for data hiding; a respective disclaimer SHOULD be shown to the HCP</p> <hr/> <p>The HCP MUST additionally consider the source coded document because this MAY contain additional information</p> <hr/> <p>Not all sections of the patient summary are provided Partial Delivery: It must be assessed if partial delivery conditions could be signaled on the content level (within the documents) instead of transmitting such information on the transaction level.</p> <hr/> <p>The computation of the CDA encoded patient summary was not approved by an HCP; a respective disclaimer MUST be shown to the HCP</p>

6.5.1.3 *epSOS Order OrderService (ePrescription)*

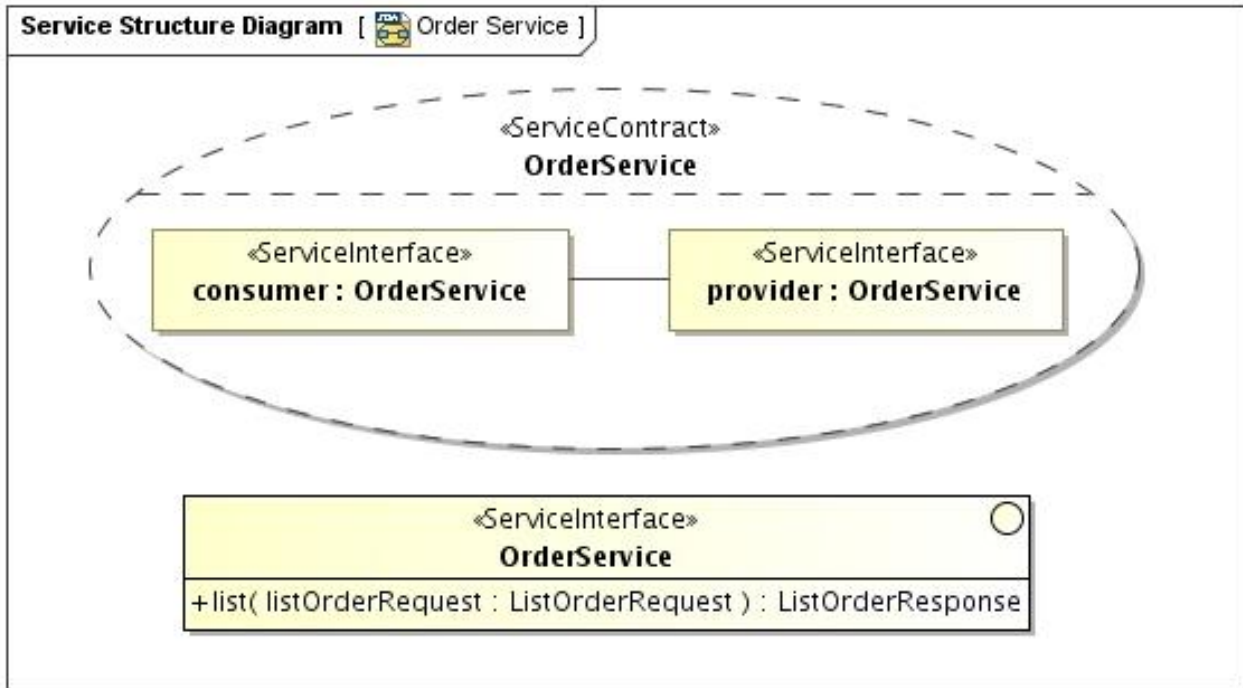


Figure 51: Order Service ePrescription

This service is used to search and retrieve medicine prescription.

Operation	list()	
Description	Obtain the epSOS-encoded, available ePrescriptions of the identified patient	
Requestor	Consuming Gateway at NCP-B	
Input Message	ListOrderRequest	
	Body	Identifier of the patient whose available ePrescriptions are requested
	Security Token	X.509 Gateway Certificate
		epSOS HCP Identity Assertion epSOS Treatment Relationship Confirmation Assertion
Output Message	ListOrderResponse	



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010

in successful Case	Body	List of
		<ul style="list-style-type: none"> - epSOS-encoded ePrescriptions - original ePrescriptions (e.g. PDF/A encoded) of the identified patient <p>information on the status of this list (e. g. more ePrescriptions are available but NCP-A was unable to transform these into the epSOS pivot format)</p>
	Security Token	X.509 Gateway Certificate
Precondition of success scenario		<ol style="list-style-type: none"> 1. The requestor is able to locate the service provider 2. The certificate of the NCP-A gateway is available to the requestor. 3. The requestor is able to verify the certificate of the NCP-A gateway. 4. The NCP-A gateway is able to verify the requestor's certificate. 5. An HCP identity assertion has been issued by NCP-B and is available to the requestor 6. The NCP-A gateway is able to verify the validity of the HCP identity assertion 7. NCP-A and NCP-B agreed on a common ID for referencing to the patient 8. An TRC assertion has been issued by NCP-B and is available to the requestor 9. The NCP-A gateway is able to verify the validity of the TRC assertion
Main success scenario		<p>Actions of the epSOS Order Service provider:</p> <ol style="list-style-type: none"> 1. validate the message signature 2. verify HCP identity assertion and TRC assertion 3. extract the patient ID from the message body 4. verify that the patient has given consent to epSOS and that the consent is valid 5. retrieve the patient's available ePrescriptions 6. enforce national security policy and (if available) patient privacy policy 7. verify authenticity and integrity of the ePrescriptions 8. transform ePrescriptions into epSOS pivot format (if requested and needed) 9. render PDF from the source document (if requested and needed) 10. sign the response message and send it to the requestor
Fault		<p>Preconditions for a success scenario are not given</p> <hr/> <p>Requestor has insufficient rights to access the patient's ePrescriptions</p> <hr/> <p>No patient summary is available for the identified patient</p> <hr/> <p>The patient summary cannot be provided in the requested encoding</p> <hr/> <p>Temporary failure (e. g. authenticity verification cannot be performed due to a PKI failure)</p>
Warning		<p>Country A allows for data hiding; a respective disclaimer SHOULD be shown to the HCP</p> <hr/> <p>Mandatory fields have been nullified for some of the provided ePrescriptions (minimum dataset is not fully provided); the HCP MUST additionally consider the source coded document</p> <hr/> <p>More ePrescriptions MAY be available but are not accessible</p> <hr/> <p>The computation of the CDA encoded ePrescription documents was not approved by an HCP; a respective disclaimer MUST be shown to the HCP</p>
		<p>Partial Delivery: It must be assessed if partial delivery conditions could be signaled on the content level (within the documents) instead of transmitting such information on the transaction level.</p>

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

Implementation recommendations²⁸

The copy of the original prescription and of the original eDispense can either be a PDF/A-1b copy of the original eP and eD or the same data elements that are sent to the asking MS, without any semantic transformation. Hence there are 2 options of implementation:

- § In the first case, the PDF contains all fields of a country A prescription,
- § In the second case, country A sends the epSOS eP data elements twice : one in epSOS format and another in the original format.

6.5.1.4 DispensationService

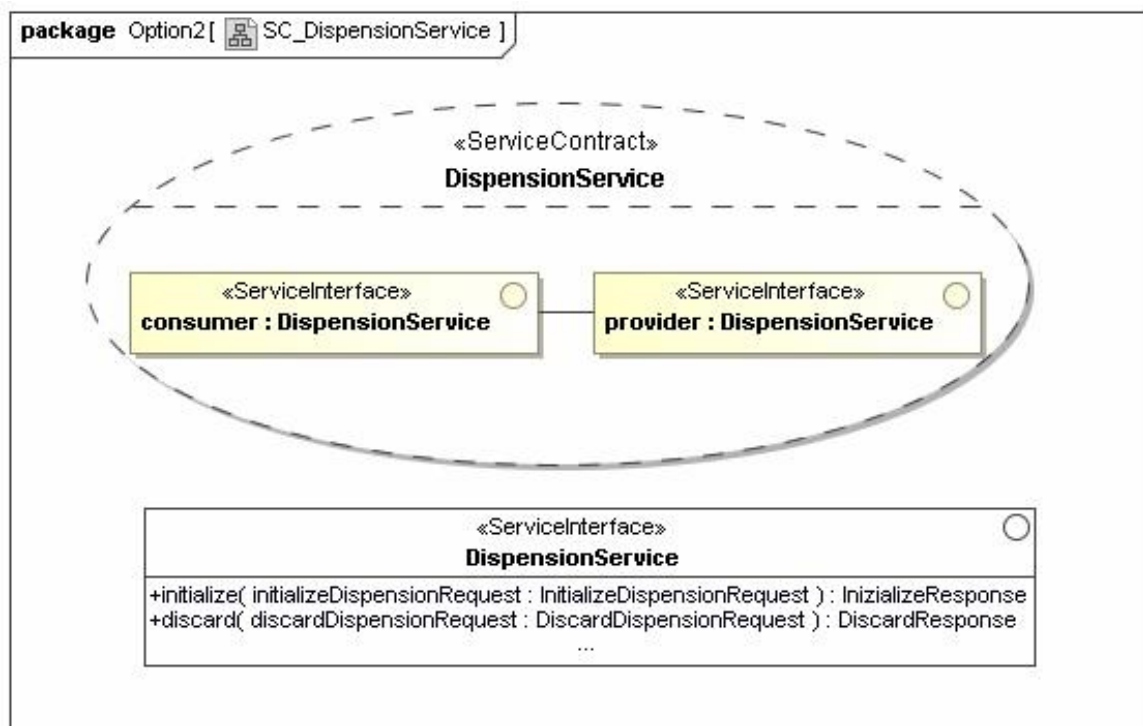


Figure 52: Dispensation Service

²⁸ Implementation recommendation targets the interface specifications then MS can decide to follow WP 3.8-3.9 JWG platform specific recommendation for its NCP development.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010
WP3.3: System architecture		

This service is used to notify information about medicine supplied.

The Initialize() operation is used to notify (send) a document from an NCP gateway in response to a document create in an internal system (HCP(O)). The document is “initialized” in order to be shared across the epSOS network (only with Patient home for epSOS context).

The discard() is used to roll-back a possible corrupted operation (either physically or logically deleting records from the underlying source) that could affect existing medical data. This operation does not come from a business requirement but is here for information system use only.

Operation	initialize()	
Description	Notify the patient’s country of affiliation on a successful dispensation of an ePrescription	
Requestor	Consuming Gateway at NCP-B	
Input Message	initializeDispensationRequest	
	Body	eDispensation dataset as defined by D3.5.2. This dataset contains a reference to the dispensed ePrescription document.
	Security Token	X.509 Gateway Certificate epSOS HCP Identity Assertion epSOS Treatment Relationship Confirmation Assertion
Output Message in successful Case	initializeDispensationResponse	
	Body	empty
	Security Token	X.509 Gateway Certificate
Precondition of success scenario	<ol style="list-style-type: none"> 1. The requestor is able to locate the service provider 2. The certificate of the NCP-A gateway is available to the requestor. 3. The requestor is able to verify the certificate of the NCP-A gateway. 4. The NCP-A gateway is able to verify the requestor’s certificate. 5. An HCP identity assertion has been issued by NCP-B and is available to the requestor 6. The NCP-A gateway is able to verify the validity of the HCP identity assertion 7. NCP-A and NCP-B agreed on a common ID for referencing to the patient 8. An TRC assertion has been issued by NCP-B and is available to the requestor 9. The NCP-A gateway is able to verify the validity of the TRC assertion 	



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010
WP3.3: System architecture		

Main success scenario	Actions of the epSOS Dispensation Service provider: <ol style="list-style-type: none"> 1. validate the message signature 2. verify HCP identity assertion and TRC assertion 3. extract the ePrescription ID from the message body 4. verify that the patient has given consent to epSOS and that the consent is valid 5. enforce national security policy and (if available) patient privacy policy 6. perform activities acc. to country-A dispensation regulations 7. sign the response message and send it to the requestor 				
Fault Conditions	<hr/> <hr/> <hr/> <hr/> <hr/>				
Operation	<code>discard()</code>				
Description	Notify the patient's country of affiliation on an erroneous creation of an eDispensation				
Requestor	Consuming Gateway at NCP-B				
Input Message	discardDispensationRequest <hr/> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Body</td> <td>eDispensation dataset as defined by D3.5.2. This dataset contains a reference to the dispensed ePrescription document.</td> </tr> <tr> <td>Security Token</td> <td>X.509 Gateway Certificate epSOS HCP Identity Assertion</td> </tr> </table>	Body	eDispensation dataset as defined by D3.5.2. This dataset contains a reference to the dispensed ePrescription document.	Security Token	X.509 Gateway Certificate epSOS HCP Identity Assertion
Body	eDispensation dataset as defined by D3.5.2. This dataset contains a reference to the dispensed ePrescription document.				
Security Token	X.509 Gateway Certificate epSOS HCP Identity Assertion				
Output Message in successful Case	discardDispensationResponse (conforms to response message; see section 4.2) <hr/> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Body</td> <td>empty</td> </tr> <tr> <td>Security Token</td> <td>X.509 Gateway Certificate</td> </tr> </table>	Body	empty	Security Token	X.509 Gateway Certificate
Body	empty				
Security Token	X.509 Gateway Certificate				
Precondition of success scenario	<ol style="list-style-type: none"> 1. The requestor is able to locate the service provider 2. The certificate of the NCP-A gateway is available to the requestor. 3. The requestor is able to verify the certificate of the NCP-A gateway. 4. The NCP-A gateway is able to verify the requestor's certificate. 5. An HCP identity assertion has been issued by NCP-B and is available to the requestor 6. The NCP-A gateway is able to verify the validity of the HCP identity assertion 				



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

Main success scenario **Actions of the epSOS Dispensation Service provider:**

1. validate the message signature
2. verify HCP identity assertion
3. extract the ePrescription ID from the message body
4. discover the patient the ePrescription was issued for
5. verify that the patient has given consent to epSOS and that the consent is valid
6. enforce national security policy and (if available) patient privacy policy
7. verify that is was the requestor who previously dispensed the ePrescription
8. perform activities acc. to country-A dispensation regulations
9. sign the response message and send it to the requestor

Fault Conditions

6.5.1.5 ConsentService

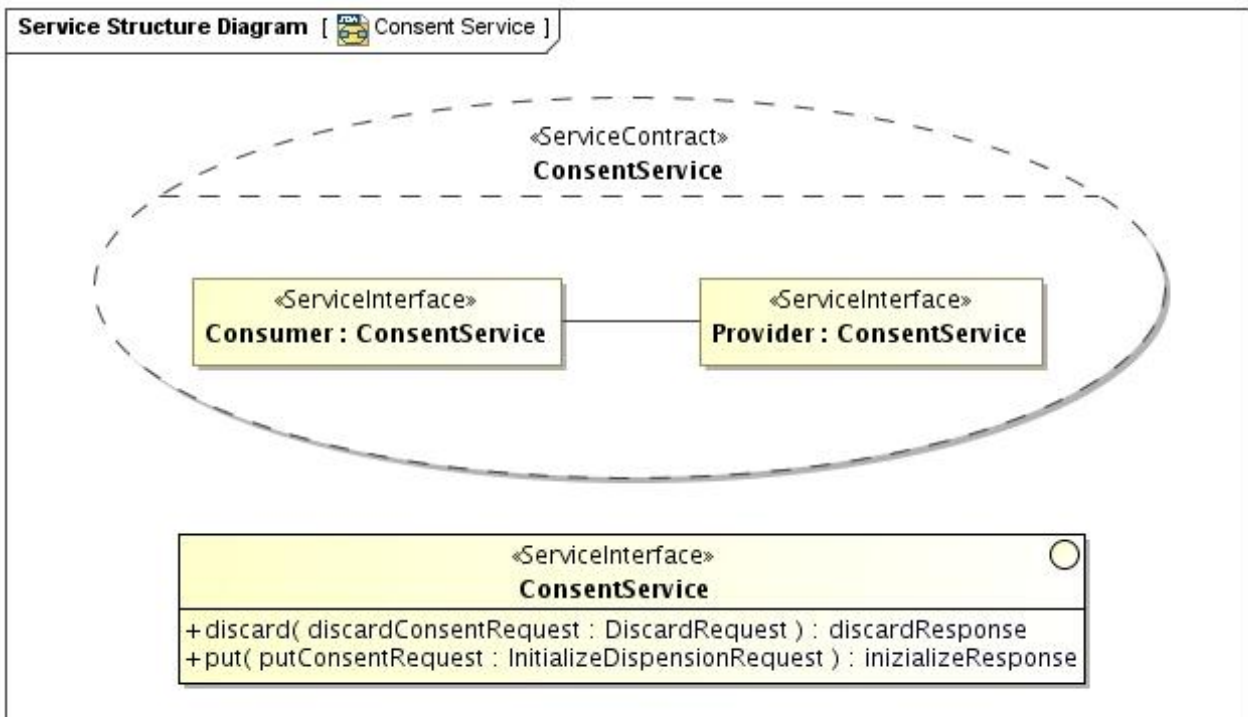


Figure 53: Consent Service



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010
WP3.3: System architecture		

This service is used to notify consent documentation to the country the patient belongs to, in order to allow national infrastructure to suitably update data access policies for that patient. Patient MAY give (put) or revoke consent (discard) in country B. In this case the consent statement is transmitted to country A. The consent giving/revoking is only valid for country B. A consent given in A is confirmed by the authorization of a HCP/O by the patient to access his data. This is an explicit activity. The already specified confirmation assertion will be used for this purpose. There is no need to transmit a consent document from country A to country B.

Operation	put ()	
Description	Notify the patient's country of affiliation on a consent newly given in the country of care	
Requestor	Consuming Gateway at NCP-B	
Input Message	putConsentRequest	
	Body	Information on the newly given consent
	Security Token	X.509 Gateway Certificate epSOS HCP Identity Assertion epSOS Treatment Relationship Confirmation Assertion
Output Message in successful Case	putConsentResponse	
	Body	Status of the consent (accepted/rejected)
	Security Token	X.509 Gateway Certificate
Precondition of success scenario	<ol style="list-style-type: none"> 1. The requestor is able to locate the service provider 2. The certificate of the NCP-A gateway is available to the requestor. 3. The requestor is able to verify the certificate of the NCP-A gateway. 4. The NCP-A gateway is able to verify the requestor's certificate. 5. An HCP identity assertion has been issued by NCP-B and is available to the requestor 6. The NCP-A gateway is able to verify the validity of the HCP identity assertion 7. NCP-A and NCP-B agreed on a common ID for referencing to the patient 8. An TRC assertion has been issued by NCP-B and is available to the requestor 9. The NCP-A gateway is able to verify the validity of the TRC assertion 	
Main success scenario	Actions of the epSOS Consent Service provider: <ol style="list-style-type: none"> 1. validate the message signature 2. verify HCP identity assertion and TRC assertion 3. extract the consent information from the message body 4. enforce national security policy and (if available) patient privacy policy 5. perform activities acc. to country-A consent regulations 6. sign the response message and send it to the requestor 	
Fault Conditions		



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

Operation **discard()**

Description **Notify the patient's country of affiliation on the revocation of a consent (revocation only affects the recent country of care)**

Requestor **Consuming Gateway at NCP-B**

Input Message **discardConsentRequest**

Body **Empty**

Security Token **X.509 Gateway Certificate**
epSOS HCP Identity Assertion
epSOS Treatment Relationship Confirmation Assertion

Output Message in successful Case **discardConsentResponse**

Body **Status of the consent revocation (accepted/rejected)**

Security Token **X.509 Gateway Certificate**

Precondition of success scenario **1. The requestor is able to locate the service provider**
2. The certificate of the NCP-A gateway is available to the requestor.
3. The requestor is able to verify the certificate of the NCP-A gateway.
4. The NCP-A gateway is able to verify the requestor's certificate.
5. An HCP identity assertion has been issued by NCP-A and is available to the requestor
6. The NCP-A gateway is able to verify the validity of the HCP identity assertion
7. NCP-A and NCP-B agreed on a common ID for referencing to the patient
8. An TRC assertion has been issued by NCP-A and is available to the requestor
9. The NCP-A gateway is able to verify the validity of the TRC assertion

Main success scenario **Actions of the epSOS Consent Service provider:**
1. validate the message signature
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. perform activities acc. to country-A consent regulations
6. sign the response message and send it to the requestor

Fault Conditions



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

Implementation recommendations

Consent Service works from B to A there is no need to transmit a consent document from country A to country B, as stated in REQ 3.3.19.

6.6 Security Architecture

The security Architecture of epSOS is based on Trust and Communication Relationships between Inbound and Outbound Gateways. The concept of trust is pivotal in epSOS. Services are set up through the network as a basis for secure messaging. The epSOS circle of trust means that service providers join together in order to exchange authentication information. This circle of trust contains an identity provider, a service that maintains and manages identity information. Transaction epSOS-1 specification from WP3.4 sets the rules for the trust establishment; Audit Trails (epSOS-2) is also part of the circle of Trust, as a guarantor for all epSOS Transaction. D3.7.2 defines a secure channel that is made up from a VPN and TLS please see D3.7.2 document.

6.6.1 Trusted Federation of NCPs

NCPs are implemented federally in order to allow for a virtual integration of autonomous sources of medical data and identity information. 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 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 HCPs is decentralized. Authentication of a HCP can only be done on the NCP that recognizes this HCP. The existence of a



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

treatment relationship between a patient and a HCP can only be attested within the legal framework of the PoC. With epSOS HCP authentication and treatment relationship attestation is always performed by the NCP where the PoC connects to.

The epSOS “Circle of Trust” (CoT) 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. A *providing gateway* operates the Web Service Endpoint (WSE) of the service provider. Each gateway is operated under the legal responsibility of an NCP.

6.6.1.1 NCP certificates

It is assumed that a list of valid NCP certificates is distributed as part of the epSOS configuration. Certificate verification is performed within the NCP by checking whether the certificate is registered with this list or not. Status validation is done by either OCSP or CLS (depending on what protocols the CA offers).

6.6.2 **Message exchange 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. The trusted node infrastructure implements the core epSOS security services which ensure the confidentiality of medical data transmission and the availability and authenticity of epSOS services. The following layers compose the message exchange Infrastructure:

Document Short name:	D3.3.2
Version:	1.4
Date:	30/04/2010

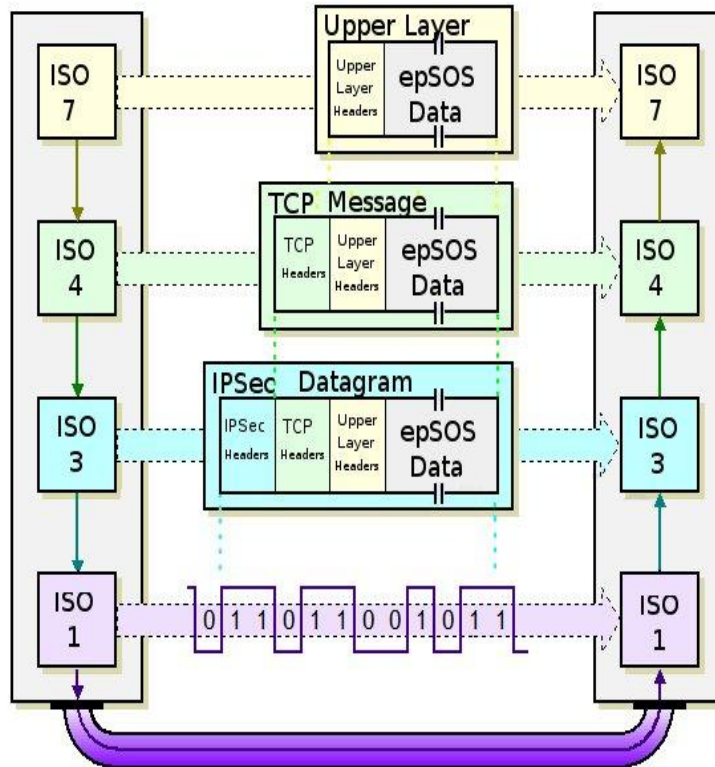



Figure 54: Message exchange layers

6.6.3 Upper Layer (Iso 7)

The upper layer support the message exchange mechanisms for the implementation of epSOS business. Security elements for the standardised enveloping of data and documents are also added. They include:

- transmission of authenticated HCP attributes under SAML Assertion,
- common message format between service as described previously through service exchanges,
- signature on message elements for auditing and brokering of document authenticity claims

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

6.6.3.1 Transmission of authenticated HCP

The *HCP Identity Assertion* is a means of user identity. This enables relying parties to run their business tasks without identifying the requester since this is done by a trusted third-party authentication service. Those assertions are encoded as SAML assertions [SAML 2.0], organised under a structured elements. They do also include a signature which references the security certificate

6.6.3.2 Common message format

The epSOS Common Message Format is a SOAP 1.2 message contained as the Body of an HTTP 1.1 [RFC2616] 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

The encoding of the containing XML document MUST be set to UTF-8²⁹.


All epSOS SOAP messages MUST comply with the WS-I Basic Profile 1.1 [BP11].

All epSOS SOAP messages MUST comply with the WS-I Secure Basic Profile 1.0 [BSP10]. All epSOS SOAP message MUST be described in a WSDL 1.1 Service Description. All WSDL type definitions MUST be in XML Schema format.

6.6.3.3 Signature on message

When auditing and brokering documents the signature is used to proved the authenticity of messages, and it is base on an x509 certificate.

²⁹ 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.

	D3.3.2_v1.4	Document Short name:	D3.3.2
		Version:	1.4
	WP3.3: System architecture	Date:	30/04/2010

6.6.4 **TCP Message Layer (Iso 4)**

Transport Layer Security MUST be supported by the epSOS network. Transport Layer Security (TLS) are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. For a mutual authentication every node must validate the certificate of the other node.

NCP-B SSL certificate and NCP-A SSL certificate MUST be used to establish a TLS v1.0 [RFC 2246] connection between country B and A NCPs.

6.6.5 **IPsec VPN Network Layer (Iso 3)**

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 pakets and SHOULD NOT exceed 4GB.

Algorithms and key lengths MUST be used. Gateway certificates MUST comply with the certificate profiles . 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]).


IPsec mechanism is epSOS application independent (Transparent to user). I do provide access control, data origin authentication and data confidentiality.

6.6.6 **Physical Infrastructure Layer (Iso1)**

This layer is responsible for moving bits between two NCPs. The communication is done from NCP to NCP. It is part in the figure to illustrate the basis of epSOS communication.

6.6.7 **Regarding the use of Certificates and PKI (Security Annex II of D3.7.2)**

It is assumed that a list of valid NCP certificates is distributed as part of the epSOS configuration. Certificate verification in performed within the NCP by checking whether the

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

certificate is registered with this list or not. Status validation is done by either OCSP or CLS (depending on what protocols the CA offers).

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).

Countries participating in circle of trust MAY agree to choose another algorithm catalogue as long as this does not fall behind [ECRYPT-II D.SPA.57] level-5.

Only non-patented hash algorithms of the SHA-2 family MUST be used.

SSL client authentication certificates must be Common PKI compatible.

6.6.8 **Regarding Node authentication**

D3.4.2 specifies according the ITI-19 transaction specification the following constraints :

- Data.Algorithms and key lengths MUST be used.
- The node certificates MUST comply with the epSOS Node Authentication Certificate Profile
- 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]).

6.6.9 **Regarding SAML Assertions**

SAML Assertions is an **XML**-based standard for exchanging **authentication** and **authorization** data between **security domains**, that is, between an *identity provider* (a producer of assertions) and a *service provider* (a consumer of assertions).

- A SAML assertion attest the authenticity of the user and the existence of a treatment relationship (refer to chapter 2 from WP34_D342_FHGISST_V-IHE-0.20.doc).
- A SAML assertions attest the HCP Identity Assertion.
- An element MUST link two assertions For instance, the presence of the patient-id and sender-vouches means the presence of a treatment assertion.
- In case of emergency MS can decide to add in the treatment relationship assertion an emergency indicator.

6.6.10 Regarding SOAP faults

SOAP faults: A three different level errors type had been identified in order to handle errors at the appropriate level of abstraction. They are described in the following figure:



Figure 55: Soap faults

6.6.10.1 Message processing fault

- 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 front-end tiers of the NCP-A. 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.

6.6.10.2 Business processing / request faults

- Error Messages in the SOAP response body: Error reporting mechanisms of the business level protocol 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. Failures usually either originate at the PoC 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.

6.6.10.3 Clinical processing / content faults

- Error messages related to the creation of the document content. There may be cases where failure may result in some elements of clinical information missing for example 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.

6.6.11 **Security zone from WP 3.7**

D3.7.2 (Section II, chapter 5) exposes how message exchanges within the epSOS architecture are treated in regard to security (referred to as “End-to-End Security”). It is out of scope of WP3.3 to cover this topic, nonetheless, a sum-up figure taken out from D3.7.2 can help to reader to reference.

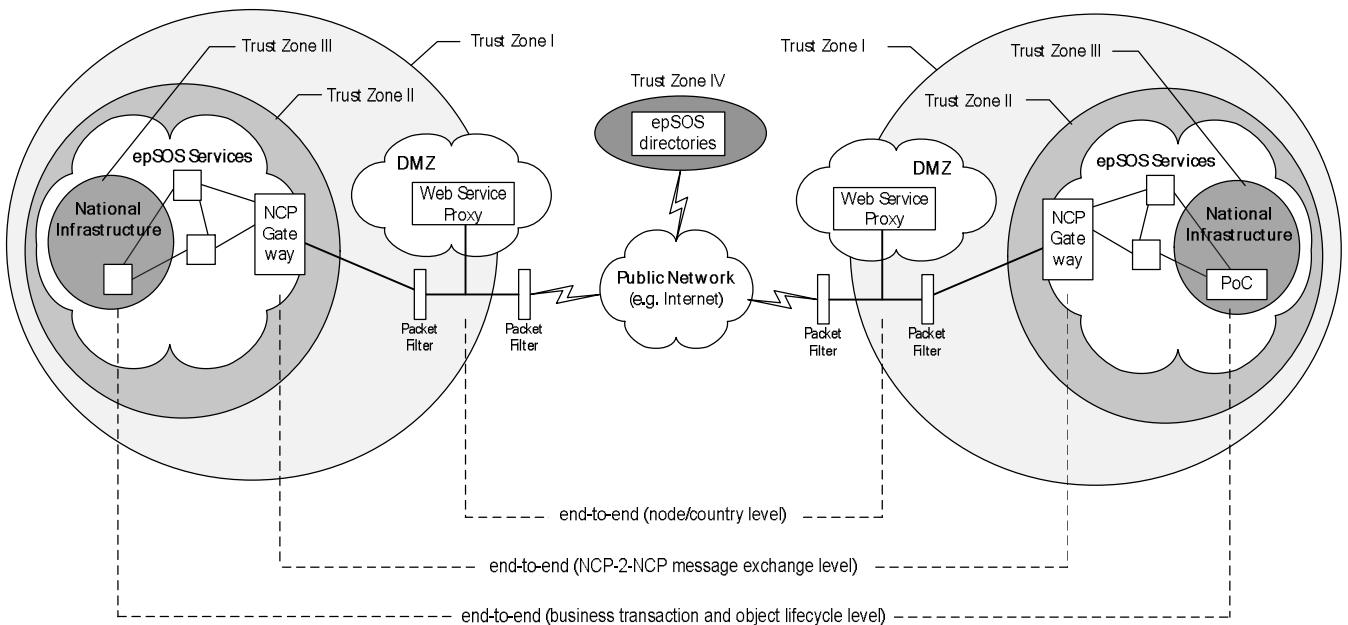



Figure 56: End-to-End security and Trust Zones (WP3.7)

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

Access Control Security Service is also taken care of in D3.7.2 (section II, chapter 2). Notably, it gives highlights to the use of XACML (eXtensible Access Control Markup Language) for epSOS when considering access policy.

6.6.12 *Session context*

Considering the potential number of exchanges for the LSP (epSOS), a stateless processing **MUST** be used at business level. Explicit sessions³⁰ with session identifiers exchanged for the application layer are out of scope.

In country B, a session in epSOS consists:

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

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

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

³⁰ A session is a logical connection between service provider and service consumer extending over multiple exchanges by maintaining state of the security context on both sides



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture


Date: 30/04/2010

6.6.13 *Adopted Standards*

This table provides a summary of the port level requirements for message integrity, authentication and confidentiality used for each of the Request and Response methods between the secured entities³¹.

Sender à Receiver	Operation	Message	Message Integrity	Authentication	Confidentiality	Algorithm
NCP A à NCP B	findIdentity ByTraits	FindIdentityByTraitsRequest	NCP X.509: UNT, Timestamp	UNT-user	NCP X.509: Body, Signature	see D3.7.2
NCP B à NCP A	findIdentity ByTraits	findIdentityByTraitsResponse	NCP X.509: Body		R X.509: Body, Signature	see D3.7.2
NCP A à NCP B	initialise	initializeRequest	NCP X.509: Body, UNT, Timestamp	UNT-user	R X.509: Body, Signature	see D3.7.2
NCP B à NCP A	initialise	InitialiseResponse			R X.509: Body, Signature	see D3.7.2
NCP A à NCP B	put	PutRequest	NCP X.509: Body, UNT, Timestamp	UNT-user	R X.509: Body, Signature	see D3.7.2
NCP B à NCP A	put	PutResponse			R X.509: Body, Signature	see D3.7.2
NCP A à NCP B	list	ListRequest	NCP X.509: UNT, Timestamp	UNT-user	R X.509: Body, Signature	see D3.7.2
NCP B à NCP A	list	ListResponse	NCP X.509: Body		R X.509: Body, Signature	see D3.7.2
NCP A à NCP B	discard	DiscardRequest	NCP X.509: UNT, Timestamp	UNT-user	R X.509: Body, Signature	see D3.7.2
NCP A à NCP B	discard	DiscardResponse	NCP X.509: Body		R X.509: Body, Signature	see D3.7.2

³¹ This representation has been derived from SCM Security Architecture document developed by the WS-I Sample Applications team.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

The Message Integrity column (i.e. which parts of the message need to be signed in each case) is explained here:


- § “UNT” (UserNameToken) – The wsse:UsernameToken element in the WS Security header containing the identity of the user who originally made the request as defined in the UsernameToken profile of WSS10 (see <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf>)
- § “Timestamp” – The wsu:Timestamp element added to the message when it was created as defined in WSS10
- § “Body” – This is the part of the SOAP message (e.g. soap:Body) that contains the business document

The Authentication column consists of the following entries:

- § [“UNT-user,”] “Cert Auth”
- § UNT-user is a UserNameToken as defined in WSS10 but without a password, i.e. it contains a UserName only. It identifies the original user that issues the request.
- § Cert Auth indicates that authentication consists of an examination of the public key certificate whose private key was used to sign the message.

The Confidentiality column indicates whether or not the message is encrypted. It contains one of the following:

- § “None”. The security analysis concluded that confidentiality was not required
- § Certificate “.” MessageParts. In which case confidentiality was applied as described below.
- § Certificate identifies the public key which is used to encrypt the symmetric key which is used to encrypt the various parts of the message. Its structure and semantics is the same as “Certificate” as defined under Message Integrity except that the certificate is being used for encryption rather than signing.
- § Message Parts are a list of the parts of the message that are encrypted. Each part is encrypted separately. It may contain some combination of: “Body”, “Start Header” and “Signature”. “Signature” means the digital signature that results from signing the message is encrypted.

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

The Algorithm column describes the cryptographic algorithms used if the message is signed or encrypted. Algorithms Key, Data and Digest must follow D3.7.2 recommendations.

- § “Key”: Asymmetric Algorithm identifies the algorithm used to generate public/private key pairs. In the Sample Application it is used to generate and verify signatures as well as to encrypt and decrypt the symmetric key used to encrypt and decrypt the message content. (See also <ftp://ftp.rsasecurity.com/pub/pkcs/ascii/pkcs-1.asc>)
- § “Data”: Symmetric Algorithm identifies the algorithm used for encrypting and decrypting the message content. (See also <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>).
- § “Digest”: Secure Hash Algorithm identifies the algorithm used for calculating the unique fingerprint for each of the signed parts of the message. (See also http://www.itl.nist.gov/div892/iip_pubs/draft-ietf-ipsec-ciph-sha-256-01.txt).



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
	Date:	30/04/2010
WP3.3: System architecture		

6.7 Profile and Transaction Mapping

The purpose of this section is to map the technical components with the epSOS transactions from WP3.4.

Technical components	Reference epSOS Transactions
InboundProtocolTermination	Query Medical Data [epSOS-7] Retrieve Medical Data [epSOS-8] Notify Medical Data Processing [epSOS-9] epSOS-12: Patient ID Discovery
OutBoundProtocolTerminator	Query Medical Data [epSOS-7] Retrieve Medical Data [epSOS-8] Notify Medical Data Processing [epSOS-9] epSOS-12: Patient ID Discovery
WorkflowManager	Query Medical Data [epSOS-7] Retrieve Medical Data [epSOS-8] Notify Medical Data Processing [epSOS-9] epSOS-12: Patient ID Discovery
TransformationManager	Retrieve Medical Data [epSOS-8] Notify Medical Data Processing [epSOS-9]
AuditTrails	Format Audit Trail [epSOS-5]
TymeSyncManagerMediator	Maintain Time [epSOS-3]
RoutingManager	Get Resource URL [epSOS-2] Get Resource [epSOS-4]
NationalConnector	n/a
SignatureManager	Attest Authenticity [epSOS-10] Retrieve CRL [epSOS-15] Verify Certificate Status [epSOS-16]
SemanticServicesImpl	n/a



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

7. Terminology and Glossary

7.1 Wording conventions

Expression	Meaning	Conveyed Sense
Must	Is obliged to	Required / Mandatory
Must not	is not allowed/permitted/acceptable/permissible is required to be not is required that ... be not is not to be...	
Should	it is recommend that it is desirable to	Best Practice / Recommendation / Left to the assessment of the country
Should not	is not recommended it is not desirable to	
May	option, but not mandatory, that should be used of the country wishes so	Acceptable / Permitted
Need not	it is not required that no ... is required	

7.2 epSOS Glossary

The following glossary is extracted from the project glossary found on Project Place³² :

Access : 1. Capability and opportunity to gain knowledge of or to alter information or material. 2. Ability and means to communicate with (i.e. input to or receive output from), or otherwise make use of any information, resource, or component in a system. Access control The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities

³² <https://service.projectplace.com/pp/pp.cgi/r368699604>



D3.3.2_v1.4

Document Short name: D3.3.2

Version: 1.4

WP3.3: System architecture

Date: 30/04/2010

Architecture : Structure and organization of a computer's hardware or system software.

Attribute : Property or a characteristic of an entity

Audit : Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures

Authentication : Formalized process to create a validated identity for a claimant, based on the value of one or more attributes of its identity.

Note: Authentication typically involves the use of a policy to specify a required level of assurance in the result after a successful completion of the process

Authenticity : The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorization : Process to approve a temporary granting of a set of privileges to an entity. The privileges enable the entity to access to some sources or to use some services of a system. Authorisation is based on policy rules for permitting an activity in a particular system

Availability : The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.

Component : Software that can be installed or replaced only as an entity to create a scalable implementation (e.g component can provide



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

directory services, data storage, provisioning..etc)

Confidentiality : The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Country A : This is the country which holds information about a patient, where the patient can be univocally identified and his data may be accessed.

Country B : This is the country, different from country A in which information about a patient is needed in case that the patient needs healthcare.

Dispenser : Health Care Professional who provides the order of a ePrescription. The professional person must be authorized to do so.

Infrastructure : Underlying base or foundation structures needed to connect to wired devices.

eDispense : Electronic object used for retrieving a prescription and giving out the medicine to the patient as indicated in the corresponding ePrescription. Once the medicine is dispensed, the dispenser shall report via software the information of the dispensed medicine(s).

EHR : **Electronic Health Record** means a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes

EHRs : **Electronic Health Record System** means a system for recording, retrieving and manipulating information in electronic health records

eP : **Electronic ePrescription ("ePrescription")** means a medicinal



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

ePrescription, provided in electronic format: "A ePrescription is understood as a set of data like drug ID, drug name, strength, form, dosage, indication or as a list of drugs together covering the patients current medicine. The dataset might differ slightly between the countries. In the context of epSOS, this definition of ePrescription will apply. However, it is not excluded that the use of the infrastructure and the service developed in epSOS might be afterwards extended to handle ePrescriptions different from medicinal ePrescriptions.

Function : Set of inputs, behaviour and outputs of a system.

Gateway : A **gateway** is a point of entry or exit. It refers to a technical object such as the technical implementation of an NCP. Requesting gateways act on behalf of a HCP (at a PoC) who requires access to a patient's medical data through epSOS. Responding gateways act as service brokers of an epSOS data provider.

HCP : "Health Care Professional" means a doctor of medicine or a nurse responsible for general care or a dental practitioner or a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC . This means that a Health Care Professional is a person who delivers health care or care products professionally to any individual in need of health care services, in order to prevent, relieve or treat a medical problem. A Health Care Professional must be related to at least one HCPO (see below).

HCPO : Health Care Provider Organization is an institution, authorized to



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

provide health care services, univocally identified in the set of the Health Care Institutions. Examples: Health Center / Hospital / Medical Emergency Vehicle / Medical Practice / Pharmacy

Integrity : The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Identification : Process to determine that presented identity information associated with a particular entity is sufficient for the entity to be recognized in a particular domain of applicability

Identifier : A non-empty set of attribute values that uniquely characterize an entity in a specific domain of applicability

Identity : A set of attributes related to an entity.

Note: Each entity is represented by one holistic identity, which comprises all possible information elements characterizing such entity (the attribute). Since such identity can be very large, even infinite for practical purposes only a subset of relevant attributes represents the entity. (e.g. name, address, date of birth, passport number, etc.)

Identity authority : Entity related to a particular domain of applicability that can make authoritative assertions on the validity of one or more attribute values in an identity

Identity information : Set of values of attributes in an identity

Identity provider (IdP) : Entity that makes available identity information and entity that operates the functions necessary to complete authentication

Note: A verifier may be the same as or act on behalf of the entity that controls identification of entities for a particular domain of applicability

Interoperability : The ability of two or more systems or components to exchange information and to use the information that has been exchanged.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

National Infrastructure: National infrastructure represents all entities where patient or HCP or Health Care records are managed in member states.

NCP : National Contact Points are organisations delegated by each participating country, acting as a bidirectional way of interfacing between the existing different national functions provided by the national IT infrastructures and those provided by the common European infrastructure, created in epSOS. The NCP takes care of external and internal national communication and functions in epSOS and the semantic mapping (if necessary) between information on either side. The NCP also acts as a kind of mediator as far as the legal and regulatory aspects are concerned. The NCP creates the conditions (by supporting trust, data protection and privacy) for a trusted relationship with other countries' NCPs.

Non repudiation : Is the security service by which the entities involved in a communication cannot deny having participated. Specifically the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).

Patient : Means any natural person who receives or wishes to receive health care in a Member State

Patient consent : Patient consent provided to the data controller means any freely given specific and informed indication of his/her wishes by which the data subject signifies his agreement to personal data relating to him/her being processed. NCPs should support exchange of PDF documents compliant to PDF/A-1b. The PDF document MUST be provided by MS A on request of MS B.

Patient Summary : Patient Summary is understood to be a reduced set of patient's



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

data which would provide a health professional with essential information needed in case of unexpected or unscheduled care (emergency, accident..) and in case of planned care (citizen movement, cross- organisational care path..) being its main purpose the unscheduled care.

- Point of Care (PoC) :** Any location where health care is provided.
- Prescriber :** Health Care Professional who issues a ePrescription. The professional person must be authorized to do so.
- Privacy :** The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- Profile :** Identity that contains attributes that are relevant in the interactions with one or more distinct domains of applicability by the entity associated with the identity
- Requirements :** Definition of all relevant needs (business, functional, non functional, technical and technological) for system specification and implementation.
- Role :** A role typically implies a collection of privileges to access or use resources available in a domain of applicability (the most important roles in epSOS are patient and various kinds of HCP)
- Trust Framework :** Trust Framework means an integrated framework detailing how trusted relationships may be best implemented between NCPs at the European interoperability level and incorporating standard legal requirements including those for audit mechanisms to be developed at EU level.
- Use Case :** Description of a system's behaviour as it responds to a request that originates from outside of that system. In other words, a use case describes "who" can do "what" with the system in question.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

The use case technique is used to capture a system's behavioural requirements by detailing scenario-driven threads through the functional requirements.


Validation :

Process to determine that presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular domain of applicability at a point in time

Note: validation usually involves verifying the syntax, and correctness of attribute values, controlling their validity status and matching them with the requirements to recognize an entity

VPN :

The VPN (Virtual Private Network) system which is one of the construction methods for private networks over the Internet,

	D3.3.2_v1.4	Document Short name: D3.3.2
		Version: 1.4
	WP3.3: System architecture	Date: 30/04/2010

8. Annexes

8.1 Contact List

List of contributors / editors to this document:

FHGISST:	Jörg Caumanns
GEMATIK:	Susanne Jucknath, Benjamin Horvat
ASIP Santé:	Anne-Laure Janeczek, Gil de Bejarry, Patrick Ruestchmann, Alain Périé
INSO:	Wolfgang Schramm
LOMBARDY:	Stefano Lotti, Giorgio Cangioli

8.2 Previous technical analysis

The following sections are extracted from previous documents issued by WP3.3 and WP3.4 (WP3.3-4_Status_May09_v03 and epSOS_Archi_Consolidated_Work_V0.4). They give insight on options analysis.

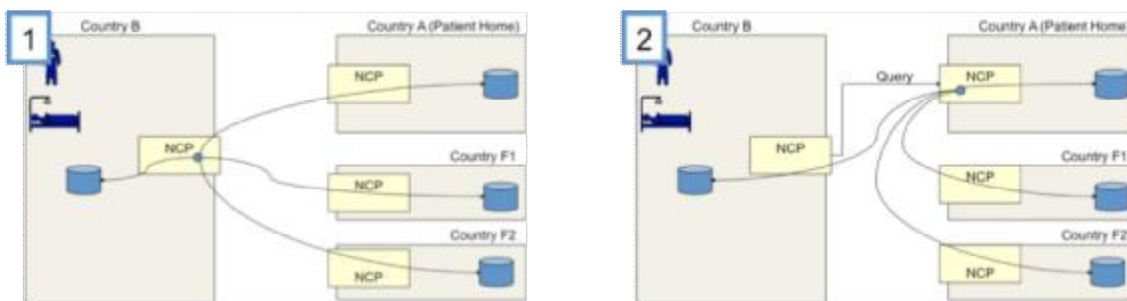
Analysis of the multiple patient data sources

This issue has been analyzed and discussed with one goal in mind: to be able to support whatever requirement WP3.2 will come to. The detailed analysis of the models (single data source, single entry point / most current data, multiple equally weighted sources) can be found in the document "WP3.3/4 Request for Discussion v0.3.

Only the conclusions are put back here:

- § all models can be tracked down to the functional requirements to be able to selectively collect data from multiple sources, apply a semantics on them and manage the list of data sources for a single patient.
- § two groups of options are defined : multicast-based (1 & 2 of figure 10) and registry-based (3 & 4 of figure 10).

- § both groups of options should be considered as valid for further elaboration from technical perspective.
- § Industry Team supported the idea that replaying multicast-based option several times against each additional country where the patient has data (with the requisite identification, authentication and authorization – specific for that country) could be a reasonable pragmatic approach for epSOS to support multi-country scenarios. A migration to option 3 (registry) would be transparent if / when countries are ready to adopt it.



Multicast-based



Multicast-based

Options to answer the Multiple Data Sources issue (source WP3.4)

All deployments and configurations presented above lead to clarify the actors:

1. A national registry/repository (part of country A's health infrastructure) which provides access to patient data managed in country A. This actor is abstract and to be instantiated by the respective national implementations. epSOS MUST NOT take any assumptions on the functionality of this actor and MUST not specify the transactions supported by this actor. epSOS MAY define safety and security assumptions on the national PS registry/repository.
2. An epSOS provider actor within each country that acts as a (reverse) proxy for the national registry/repository.



D3.3.2_v1.4	Document Short name:	D3.3.2
	Version:	1.4
WP3.3: System architecture	Date:	30/04/2010

3. A national consumer which is part of country B's health service infrastructure. This actor is abstract and to be instantiated by the respective national implementations. epSOS MUST NOT take any assumptions on the functionality of this actor and MUST not specify the transactions supported by this actor. epSOS MAY define safety and security assumptions on the national consumers.
4. An epSOS consumer actor which acts as a proxy for the national consumer actor.
5. A Discovery Actor which is responsible for discovering patient data within other countries.
6. A Gathering Actor which is responsible for gathering the discovered medical data of a patient.
7. A Notification Actor which sends information on PS updates / medicine dispense to the Discovery Actor.

All scenarii can be implemented by instantiating this actor by either a registry or a multicast configuration as well as by allowing the gathering actor to be deployed in either country A or B.

*** *End of D3.3.2* ***