




# Smart Open Services for European Patients

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

## Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)

WORK PACKAGE	<b>JWG 3.8/3.9</b>
DOCUMENT NAME	<b>Architecture of the National Contact Point (NCP) "In A Box"</b>
SHORT NAME	<b>NCP - HLDD</b>
DOCUMENT VERSION	<b>1.0</b>
DATE	<b>14/05/2010</b>


	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>COVER AND CONTROL PAGE OF DOCUMENT</b>	
<b>Document name:</b>	<b>JWG_NCP_Architecture_HLDD</b>
<b>Document Short name:</b>	<b>NCP - HLDD</b>
<b>Distribution level</b>	<b>CO</b>
<b>Status</b>	<b>Approved</b>
<b>Author(s): Organization:</b>	<b>B.Horvat, S.Evdokimov, R.Melgaard, H.L.Nielsen, P.Loubjerg, S.Bittins, J.Caumanns, A.Estelrich, P.Ruestchmann, A.Périé, G.De Bejarry, A.Hansen, M.Kovarova, G.Heider, P.Gross, T.Pass, G.Cangioli, S.Lotti, M.Melgara, G.Orsi  JWG-Technical Core Team</b>


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.

<b>ABSTRACT</b>
<b>JWG_NCP_Architecture_HLDD provides the information concerning the possible High Level Design of the NCP-in-a-Box concept, both considered as gateway toward Country A and toward Country B. It contains general description of the NCP-in-a-Box architecture as well as details about individual components. The document is to be distributed to potential Implementers of the NCP-in-a-Box and should aid them in responding to a Request for Information.</b>

<b>Change History</b>					
<b>Version</b>	<b>Date</b>	<b>Status Changes</b>	<b>From</b>	<b>Details</b>	<b>Review</b>
V0.1	21/01/2010	Draft	Gematik	Initial Version based on minutes by JWG 3.8/3.9 (Paris, 01-19-2010)	JWG-TC
V0.2	01/02/2010	Draft	Gematik	The document has been adapted to the agreements found in Vienna F2F on 29.01.2010	JWG-WPLs
V0.3	01/02/2010	Draft	Lombardy	Converted in epSOS Template, updated ToC.	
V0.4	09/02/2010	Draft	Semantic Group	Revised the semantic content of the document	


	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

V0.41	18/02/2010	Draft	Gematik	The document has been adapted to the agreements found in TConf on 15.02.2010	
V0.45	26/02/2010	Draft	Gematik	Integration of the input provided as discussed on F2F meeting in Berlin on 18.02.2010	
V0.46	2/03/2010	Draft	Gematik	Integration of the input provided for the discussion on TConf on 2/03/2010	
V0.472	10/03/2010	Draft	Gematik/ Dig.Health	Integration of the input provided for the discussion on TConf on 8/03/2010	
V0.48	11/03/2010	Draft	Gematik	Integration of the input provided for the discussion on TConf on 11/03/2010	
V0.49	16/03/2010	Draft	Dig.Health	Integration of the input provided for the discussion on TConf on 11/03/2010	
V0.5	16/03/2010	Draft	Gematik	Integration of the input provided for the discussion on WP 3.4 TConf on 15/03/2010	
V0.52	19/03/2010	Draft	Gematik	Structural changes in Section 5 that were discussed at TConf on 19/03/2010	
0.58	20/04/2010	Draft	Gematik	Integration of the input provided during the Internal Review round	
0.59	23/04/2010	Draft	Gematik	Integration of the input provided by Giorgio	
0.60	11/05/2010	Draft	Lombardy	Review of Chapter 6 by Marcello	
1.0	14/05/2010	Draft	Digital Health/ Lombardy	Release of approved version	


	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

## TABLE OF CONTENTS

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
1.1	Background and Methodology followed .....	7
1.2	Scope of this document .....	8
1.3	Glossary .....	8
<b>2</b>	<b>Requirements and Security Considerations.....</b>	<b>10</b>
2.1	Requirements .....	10
2.2	Security Considerations.....	11
2.2.1	Identification & Authentication requirement: .....	11
2.2.2	Data integrity requirement:.....	11
2.2.3	Access Control requirement:.....	12
2.2.4	Data Confidentiality requirement: .....	12
2.2.5	Data availability requirement:.....	12
2.2.6	Non Repudiation requirement: .....	12
2.2.7	Audit & Accounting requirement:.....	12
2.2.8	Trustability requirement:.....	13
2.2.9	Environmental and operational requirement:.....	13
2.2.10	Considerations .....	14
2.3	Conclusions of the technical core team .....	14
<b>3</b>	<b>NCP-In-A-Transparent-Box .....</b>	<b>15</b>
3.1	Overview .....	15
3.2	Common Components.....	16
3.2.1	InboundProtocolTerminator .....	17
3.2.2	OutboundProtocolTerminator .....	18
3.2.3	WorkflowManager .....	18
3.2.4	Security Manager.....	18
3.2.5	TransformationManager.....	18
3.2.6	TerminologyServicesAccessManager.....	18
3.2.7	AuditTrailWriter .....	18
3.2.8	AuditRepository.....	19
3.2.9	RoutingManager .....	19
3.2.10	ConfigurationAndMonitoringManager.....	19
3.2.11	NationalConnector .....	19
3.3	EpSOS Front-End Services Transactions .....	19
3.3.1	epSOS Patient Identification Service.....	19
3.3.2	epSOS Patient Service .....	21

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

- 3.3.3 EpSOS Order Service ..... 24
- 3.3.4 EpSOS Dispensation Notification Service ..... 26
- 3.3.5 EpSOS Consent Notification Service ..... 28
- 3.4 Nation-Specific NCP Components ..... 29
- 3.5 Central Common Services Components ..... 31
- 3.6 NCP-B Internet Front-end ..... 31
  - 3.6.1 System Overview ..... 31
  - 3.6.2 Security ..... 34
  - 3.6.3 HCP Authentication ..... 35
  - 3.6.4 Site Collection ..... 38
  - 3.6.5 Application Life-Cycle ..... 39
  - 3.6.6 Page Life-Cycle ..... 39
  - 3.6.7 HCP Session Life-Cycle ..... 40
  - 3.6.8 HCP Patient (TRC) Session Life-Cycle ..... 41
- 4 Example Deployment Composition ..... 42**
  - 4.1 Navigation Paths ..... 43
    - 4.1.1 NCP-B Role ..... 43
    - 4.1.2 NCP-A Role ..... 44
    - 4.1.3 Central Common Service Role ..... 45
  - 4.2 Deployment ..... 45
  - 4.3 Implementation Platform ..... 46
  - 4.4 Security Setup for NCP ..... 46
    - 4.4.1 Security Zones ..... 46
    - 4.4.2 NCP Gateway Application ..... 50
- 5 Components Design ..... 51**
  - 5.1 Inbound Protocol Terminator ..... 51
    - 5.1.1 epSOS Patient Identification Service ..... 51
    - 5.1.2 epSOS Patient Service ..... 53
    - 5.1.3 epSOS Order Service ..... 55
    - 5.1.4 epSOS Dispensation Service ..... 57
    - 5.1.5 Consent Service ..... 60
  - 5.2 Outbound Protocol Terminator ..... 63
  - 5.3 Workflow Manager ..... 64
    - 5.3.1 Handler Interface ..... 65
  - 5.4 Audit Trail Writer ..... 65
  - 5.5 Audit Repository ..... 66
  - 5.6 Security Manager ..... 67
  - 5.7 Transformation Manager ..... 68
  - 5.8 Terminology Services Access Manager ..... 73

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

5.8.1 Interaction Uses ..... 76

5.9 Routing Manager ..... 78

5.10 Configuration And Monitoring Manager..... 79

5.11 NationalConnector ..... 80


**6 Proposals for implementation strategies for Components in Common and Components Non in Common..... 81**

6.1 NCP Implementation Strategy..... 81

6.2 Estimation of development effort of NCP-in-a-transparent-box components .... 83

6.2.1 Estimation baseline assumption..... 83

6.3 Further steps towards the Design Specification and Guidelines ..... 84

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

## 1 Introduction

### 1.1 Background and Methodology followed

The epSOS specifications have been realized as a cooperation of different Work Packages (WP). The WP3.3 (Architecture) and WP3.4 (Common Components) are responsible for defining epSOS architecture. Requirements on security are defined by WP 3.7. The functional services performed by the epSOS architecture are defined in accordance to WP 3.1 and WP 3.2 Functional Requirements on ePrescription, eDispensation (eP/eD) and Patient Summary (PS), the Patient and HCP Identification processes (WP3.6) and the Semantic Interoperability Services (WP 3.5).

All the functional and technical requirements directly derive and must be conformant to the Legal and Regulatory Requirements and the defined and signed Agreements among the MS to set up the Circle of Trust.


WP 3.8 (MS Guidelines definition) and WP3.9 (Proof of Concept definition) have continuously and actively co-operated with all the WP leaders and the TPM, adopting the following procedure for defining the High Level Design of the NCP, as described in epSOS Annex I and Deliverables:

- creation the Joint Working Group, composed by WP3.8 and WP3.9 members and the WP leaders
- definition of the Pilot scope
- identification of open issues related to implementation choices
- convergence among all the Specifications of each WP into the proposed HLDD
- finalization of the first draft of HLDD, including the rough estimation of the implementation effort
- set up of sharing and approval process of HLDD among Beneficiaries
- creation and release of consolidated version of HLDD to be used for the definition of Implementation Guidelines (WP3.8), Detailed Technical Specification and Testing tools (WP 3.9)
- definition of the Detailed Technical Specifications for the implementation and Request for Invitation and Request for Tender.

The most important part in the epSOS use case is the National Contact Point gateway (further in the text referred to as NCP), the component that is responsible for connecting national infrastructures. For the pilot phase, it was decided to identify “common components” of the NCP gateway similar for all member states (MS) which can be developed in common.

Not all functionalities of the NCP can be fulfilled by the common components. As a result, some of the functionalities require components that are specific for each MS. The focus of this implementation paper is the description of the common components.

For the pilot it was decided to build the “NCP-In-A-Transparent-Box” that is composed from the common components that implement functionality that is common for several MSs and are connected to nation-specific components implementing nation-specific processes. The resulting NCPs can be used by the MS to support their pilot sites.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name:	NCP - HLDD
		Version:	1.0
	JWG 3.8/3.9: Joint Working Group	Date:	14/05/2010

A top-down approach was used for developing this document. An emphasis was made on understanding the general architecture, followed by a more detailed description of the common elements (common components). This top down approach will also be followed when describing the Detailed Technical Specifications. The document was built in several steps:

- The common components were defined
- A core team of technical experts was identified and split into three functional groups:
  - The architecture group defining the architecture of the “NCP-In-A-Transparent-Box”.
  - The semantic group
  - The group providing detailed description of the common components

Several countries have actively participated at these activities: Austria, Denmark, France, Germany, Lombardy, Slovakia, Spain, Sweden; UK provided consultancy support.

## 1.2 Scope of this document

This document defines the architectural view on the “NCP-In-A-Transparent-Box”, describing the functionalities which are common and the “common components” implementing these functionalities. It documents which functionality can be developed in common and which “common components” will be specified.

The “Box” is defined “Transparent” because every MS can decide if it is worth for it to adopt all or only part of the components defined as potentially common.

Furthermore, it describes on a high level the national part of the “NCP-In-A-Transparent-Box”, namely the “NationalConnector”.

In order to provide a light integration solution for those MSs who at this moment do not plan a full integration the NCP Country-B functionality with their national infrastructure, the document also describes a Country B Front-end solution.


Certain functionality required by NCPs (e.g., distribution of configuration-relevant data) is to be implemented as central services and referred to as Central Common Services. The specification for the Central Common Services is not included in this document. However, the way in which the NCP will be connected to them is defined, together with the NCP component to perform the interconnection.

## 1.3 Glossary

The epSOS Glossary will not be exhaustively explained in this document. The deliverables of the preceding work packages are seen as a basis for this document.


NCP	National Contact Point is a legal entity which is responsible for the epSOS communication (see Annex I)
NCP gateway	Component under the control of the NCP that manages all epSOS transactions and which connects the national infrastructure to the epSOS backbone.



	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name:	NCP - HLDD
		Version:	1.0
	JWG 3.8/3.9: Joint Working Group	Date:	14/05/2010

NCP-In-A-Transparent-Box    A modular NCP implementation that can be used completely or partly by any MS to fulfill NCP obligations. This implementation is not mandatory.

Central Common Services    A set of central services jointly used by NCPs (e.g., e.g., distribution of configuration-relevant data).

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010


## 2 Requirements and Security Considerations

For all NCP implementations, the requirements of the current epSOS deliverables are mandatory. These are not repeated in this document. The deliverables of all technical working packages and the legal working package WP 2.1 are relevant for the NCP design and the definition of common components.

### 2.1 Requirements

The requirements of this section form the basis for the work of the technical core team.

- epSOS basic pillars have to be respected and safeguarded (cfr: D5,2,1: Initial Scope)
  - epSOS LSP will provide solutions and validate them with Pilots for Cross-border interoperability of eP and PS
  - epSOS eP and PS Cross-border interoperability must be based on a Legal and Regulatory framework which includes the signature of contractual agreements among the Member States to state the legal responsibilities and assure the adequate level of trust.
  - epSOS eP and PS Cross-border interoperability must be based on already existing National eP and PS services,
  - epSOS eP and PS Cross-border interoperability must not interfere with National eP and PS services or request modification to them
  - epSOS eP and PS Cross-border interoperability services must not decrease the level of security provided by every MS to its Citizens
  - epSOS LSP will not develop European eP / PS services, but make existing national services accessible from all participating member states
- HLDD is based on the legal requirements of WP2.1, the functional requirements of WP3.1 and 3.2, the technical requirements of WP3.3, 3.4, 3.5, 3.6, 3.7, applied to the defined Pilot Scope, taking into account deliverable harmonization and open issue solutions defined by JWC (including PD3 WP Leaders and TPM).
- NCP in a transparent box means that every component has a defined interface and if needed can be easily substituted by a corresponding national implementation. It is agreed upon that the NCP must be provided as a very flexible framework.
- As many components as possible, adopting reasonable criteria, should be developed in common. However, this will not be possible for all functionalities of the NCP.
- The possible strategies that might be followed to develop in common the NCP components and the Country-B Front-end will be described in the HLDD, however it is the responsibility of Project Coordinator and PEB/PSB to choose among alternatives and adopt the selected one.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

## 2.2 Security Considerations

epSOS Grant Agreement, Consortium Agreement and the Framework Agreement Documents have to assure the respect of the Security Requirements, regardless the fact the NCP is acting as the data controller or the data processor<sup>1</sup>.

All development has to be in line with all security requirements of the working packages and the policies of all beneficiaries.

Below, Security Requirements derived from WP3.7 are listed.

Making reference to ISO/IEC 27002, generally the main objectives of computer security can be summarized as:

- **Authenticity:** the identity of an actor has been proven as true;
- **Confidentiality:** information is accessible only to authorized users/[actors];
- **Integrity:** accuracy and completeness of information and processing methods;
- **Availability:** authorized users have access to information and associated assets when required;
- **Accountability/Non Repudiation (Liability):** each communication and each data transaction can be tracked back to a certain originator in a traceable chain of activities.

In epSOS LSP Project, the core of data processing of the epSOS NCP, is related to process Health Care data. This highly sensitive data processing imposes that the: authenticity, confidentiality, integrity, availability and liability security objectives must be guaranteed through the following suitable security requirements.

### 2.2.1 Identification & Authentication requirement:

**NCP-Req#3.7.01a (NCP identification):** a NCP MUST have a unique electronic identity in a common cryptographic domain (such as, for example, digital certificates following x509 Standard).

**NCP-Req#3.7.01b (NCP local User I&A):**

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


**NCP-Req#3.7.02 (Authenticating Network Access):** each NCP MUST ensure that all connections to remote servers (both other NCPs and local systems) and applications are authenticated.

### 2.2.2 Data integrity requirement:

**NCP-Req#3.7.03a (Digital Signatures):** if in a MS the epSOS LSP Users apply a digital signature, then the MS-related NCP MUST be able to:

- verify that the digital signature is valid (this implies that the user certificate is also valid)
- confirm that validity to any other MS-NCP, through a digital signature.

<sup>1</sup> Data Processor and Data Controller are defined in "Directive 95/46/EC, Article 2 – Definitions –". D2.1.2 provides the definition and the application within epSOS context.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

**NCP-Req#3.7.03b (Digital Signatures):** if a MS does not adopt a digital signature, then the MS-related NCP MUST be able in any case to:

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

**NCP-Req#3.7.08 (System and data integrity):** a NCP MUST ensure, by strong cryptographic mechanisms, the ability to discover if the medical information has been altered or destroyed in an unauthorized manner, so that the medical information may not be further processed.

### 2.2.3 Access Control requirement:

**NCP-Req#3.7.04 (Access Control):** a NCP MUST provide Access Control mechanisms which provide functionalities that allow, for a given User, the specification of which data and services the User can get access to, and which privileges the User has with regard to the data and services.

### 2.2.4 Data Confidentiality requirement:

**NCP-Req#3.7.05 (Confidentiality):** a NCP MUST use strong cryptographic mechanisms to prevent the unauthorized disclosure of personal medical information or security critical system data during the transfer and processing within the NCP itself if this processing has confidentiality vulnerabilities.

**NCP-Req#3.7.06 (Protecting Source and Destination Integrity during data transmission):** the source and destination of the message during data transmission between NCPs MUST be protected to maintain its integrity.

**NCP-Req#3.7.07 (Protecting Data Storage):** if storage is performed, a NCP MUST protect medical information or security critical system data it contains. The use of pseudonymization mechanisms SHOULD be used if possible or reasonable.

### 2.2.5 Data availability requirement:

**NCP-Req#3.7.09 (Availability):** NCP best effort MUST ensure the respect of the agreed Service Level Agreements as defined by WP3.1 & WP3.2 and detailed by WP3.8.


### 2.2.6 Non Repudiation requirement:

**NCP-Req#3.7.10(Non Repudiation):** a NCP MUST have a strong cryptographic mechanism (i.e. RSA) to ensure the non repudiation of each document produced by itself or messages exchanged with other NCPs.

### 2.2.7 Audit & Accounting requirement:

**NCP-Req#3.7.11 (Accounting and Control):** a NCP MUST have a mechanism to record every access request and disclosure of medical information and clinical data, together with the time and identity of the accessing User.

Clinical data MUST NOT be included in accounted data. Accounting records MUST be maintained as long as the pilot project lasts, unless otherwise legally required.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

**NCP-Req#3.7.12 (Auditing):** it **MUST** be ensured that each action which has an impact on security is recorded. If data to be recorded contain both medical and personal data, an anonymization or pseudonymization process **SHOULD** be used if possible or reasonable. In any case the recorded data **MUST** not contain personal health care data, but can contain a unique identifier to a data object. Audit records **MUST** be maintained as long as the pilot project lasts, unless otherwise legally required.

**NCP-Req#3.7.13 (fraud detection):** NCP **MUST** provide tools to discover possible frauds in the use of medical data

**NCP-Req#3.7.14 (Continuously Logging):** logging on the NCP **SHOULD** be operational at all times. In case of failure, the NCP involved **MUST** inform all the other NCPs.

**NCP-Req#3.7.15 (Securing Access to Audit/Account Logs):** a NCP **MUST** secure the access to audit records to prevent misuse or compromise.

**NCP-Req#3.7.16 (Logging Transactions):** a secure audit record **MUST** be created each time a User asks to access medical information of a Patient or to send an e-prescription dispensation's notification.

**NCP-Req#3.7.18 (Minimum Content of Accounting Logs):** the logs **SHOULD** contain:

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


**NCP-Req#3.7.19 (Reporting Every Access medical information – notifications included-):** it **SHOULD** be possible to identify all requests to access to any Patient's record(s) (dispensations and modifications included) over a given period of time according to different parameters (Users, Patients' records, etc.).

## 2.2.8 Trustability requirement:

**NCP-Req#3.7.17 (Trust):** it **SHOULD** be allowed to submit each NCP to a "second part" (see ISO 9000) security audit procedure performed by the other MS, so that it will be possible to verify the compliance with the security requirements established by the pilot sites agreement.

## 2.2.9 Environmental and operational requirement:

Besides the aforementioned security requirements it is strongly recommended that also environmental and operational epSOS NCP security requirements **SHOULD** be met by all NCPs engaged in the epSOS pilot phase. (ref. WP3.7\_D3.7.2\_Security\_Services document).

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name:	NCP - HLDD
		Version:	1.0
	JWG 3.8/3.9: Joint Working Group	Date:	14/05/2010

### 2.2.10 Considerations


As part of WP3.7 deliverables, “WP3.7\_D3.7.2\_SECTION\_II\_SECURITY\_SERVICE” describes security services that must be implemented in order to fulfil the aforementioned security requirements. It is important to note that many of the described security services are referencing various cryptographics mechanism (digital signature, encryption, hashing) as these mechanism are the commonly adopted to produce a stronger security safeguards.

It must also be noted that the same document, for specific security services (non-repudiation and audit&accounting), describes a simplified solution that could be adopted during the piloting phase.

### 2.3 Conclusions of the technical core team

To enable the development of the “NCP-In-A-Transparent\_Box” additional requirements have been defined by the technical core team. These additional requirements are listed below:

- The NCP Gateway is composed of a common (epSOS) part and an individual (nation specific) part. The components of the common part are specified in detail. The nation specific part is implemented in the “NationalConnector” that is not specified in detail but implements a stable interface that is defined by the joint working group 3.8/3.9 (JWG).
- The components in the common part might or might not be adopted by the different MSs, according to their National infrastructure and the MS defined implementation policies.
- The architecture and the epSOS transactions must be able to transport pseudonymised data that was sent by country A in a way that only pseudonymised data can be seen by NCP-B.
- The individual security requirements of each MS, derived from D3.7.2, are documented in this document in Section 2.2. Organizational and technical means must be defined in the deliverable to make sure security requirements are fulfilled. If security requirements cannot be fulfilled, this must be documented.
- The authentication of the health care professionals (HCP) is a prerequisite for any epSOS transaction (usually Identification Handshake). The authentication of the HCP is done by the identity provider which is part of the national infrastructure and must be separated from the NCP.
- The identification request is checked in the common part of the NCP A in the way that the XML containing the patient traits is schema validated; the semantics of the traits are checked in the national part.
- The security audit that forms the basis for administrative tasks and reporting must be separated from the functional logging.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

### 3 NCP-In-A-Transparent-Box

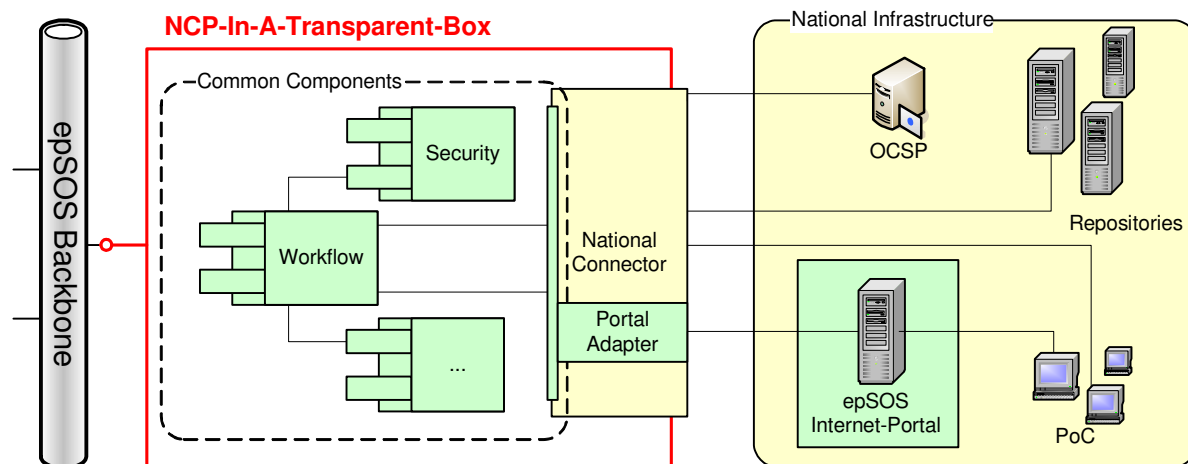
This section presents an overview of an “NCP-In-A-Transparent-Box”. First it presents the components of the NCP. Then interactions between the components are presented.

#### 3.1 Overview

Deliverable 3.3.2 describes in the Information System View the structure and the high level behaviour of the NCP gateway.

The NCP-In-A-Transparent-Box is one scenario of an NCP implementation that includes special requirements (see Chapter 2). Therefore, the composition of the NCP is slightly different from the architecture defined in Deliverable 3.3.2. The main difference is that the components are separated into “common components” and “nation-specific components” with the nation-specific components being encapsulated by the “NationalConnector”.


In order to provide a stable basis for the common components, the interface of the NationalConnector has to be defined. The NationalConnector is implemented as a black box having its subcomponents hidden from the NCP. They are nevertheless part of the NCP because they implement core functionality of the NCP and fulfill functional and non-functional requirements.



**Figure 1 NCP-In-A-Transparent-Box**

The NCP-In-A-Transparent box is meant to be a flexible framework of common components that may be used by MS to fulfill the requirements of their pilot sites and epSOS regarding the epSOS transactions. Figure 1 shows by color which components MAY be developed in common (green) and which are specific for each member state (MS).

Each member state is responsible for its own and unique implementation of the NCP gateway. We assume that for reducing the costs, each MS will try to use as many common components as possible. Nevertheless a reasonable part of the NCP gateway remains nation specific and therefore cannot be specified nor jointly developed by epSOS. The focus of this chapter lays on the common components that are defined in section 3.2.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

Common central services are not shown in that abstract figure but they will be connected to the epSOS Backbone.

The national connector encapsulates the nation-specific part of the NCP hence it is not a common component. Nevertheless it has an interface that is defined in common to achieve interoperability between the common components and the national part.

### 3.2 Common Components

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


- InboundProtocolTerminator
- OutboundProtocolTerminator
- SecurityManager
- TransformationManager
- TerminologyServiceAccessManager
- WorkflowManager
- AuditTrailManager
- RoutingManager
- ConfigurationAndMonitoringManager
- NationalConnector

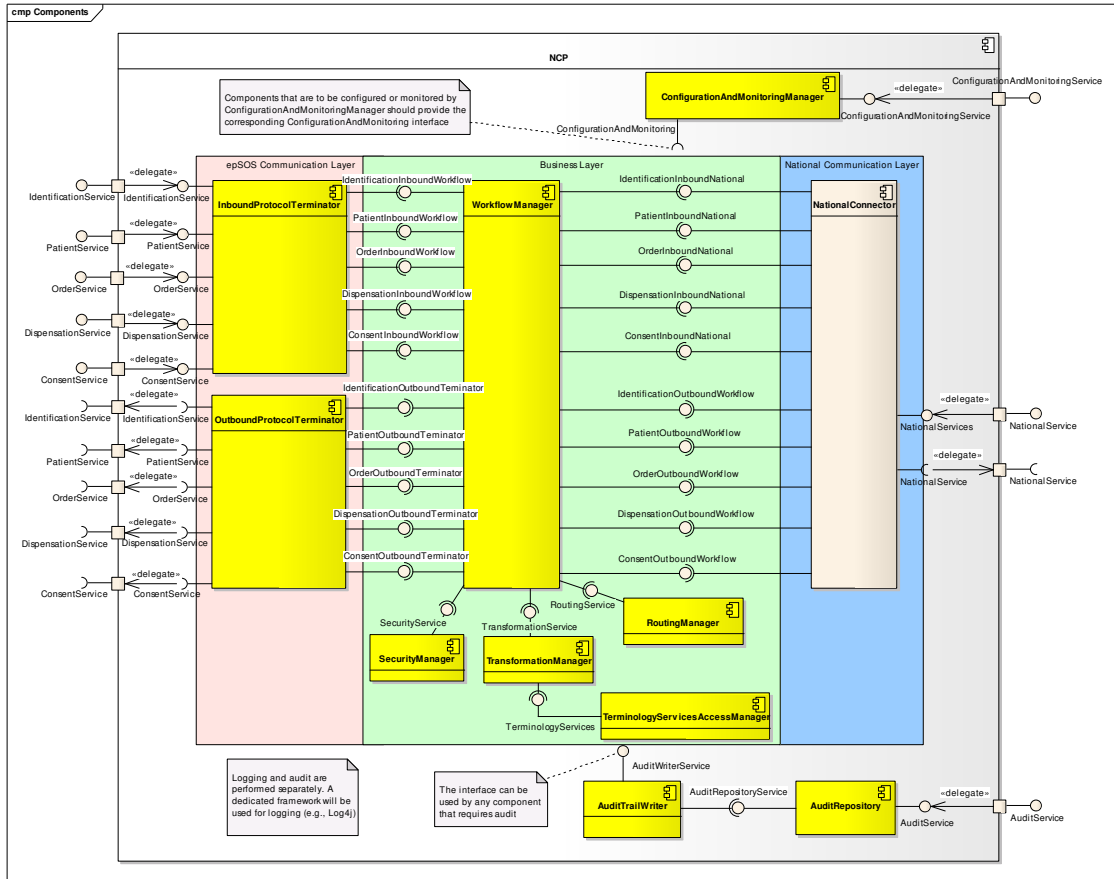
The following components were discussed but have been discarded

- Time synchronisation is done by the platform, therefore there will be no dedicated component for that task
- A LoggingManager is not needed since the logging will be processed by a dedicated logging framework. The logging that is needed for reporting and administrative tasks has to be separated from the security audit.
- There will be a management console that is used for administrative tasks, for monitoring and for reporting. The management console will be able to read the logfiles and will be able to provide the configuration data.

The definition of the components is very close to the basic architecture presented in Deliverable 3.3.2. There are, however, a number of differences that is a consequence of new requirements stated by the JWG. On the one hand, the architecture of the NCP-In-A-Transparent-Box should allow having as much of commonly developed components as possible. On the other hand, the architecture should be flexible enough for supporting the variety of national solutions implemented by MSs. An overview of the components is given in Figure 2 Common Components.



	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
	JWG 3.8/3.9: Joint Working Group	Version: 1.0
		Date: 14/05/2010



**Figure 2 Common Components**


Components that are not common but part of the NCP gateway are grouped in the NationalConnector.

The basic concepts of the architecture are derived by the logical sectioning of the NCP gateway into three sections (vertical layers). The workflow manager is the component which is responsible for managing communication between the layers.

### 3.2.1 InboundProtocolTerminator

The *InboundProtocolTerminator* plays the role of epSOS web services provider. The service is defined with a set of epSOS WSDL and a stack of security protocol such as: SSL, SAML and others (see below). These protocols have to be terminated for any incoming message in the *InboundProtocolTerminator* component. The component implements the endpoint of the epSOS services.

The *InboundProtocolTerminator* checks signatures of SOAP requests initiated by the *OutboundProtocolTerminator* of another NCP, performs deserialization of these requests into Java objects and passes them to the *WorkflowManager* by calling an appropriate operation of the corresponding interface. Once the *WorkflowManager* returns the result of the call, the *InboundProtocolTerminator* serializes it into a SOAP response, signs the response and sends it to the NCP from which the SOAP request originated.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

### 3.2.2 OutboundProtocolTerminator

The *OutboundProtocolTerminator* plays the role of epSOS web services consumer. The component serializes Java objects passed as to it by the *WorkflowManager* into SOAP requests, signs the request and transmits them to the remote *InboundProtocolTerminator* of another NCP by calling an appropriate operation of one of its service interfaces. When the response arrives, it is the responsibility of the *OutboundProtocolTerminator* to validate signatures of the response, deserialize the response and pass the resulting Java object to the *WorkflowManager*.

### 3.2.3 WorkflowManager

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

### 3.2.4 Security Manager

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

### 3.2.5 TransformationManager


This component will be called by the *WorkflowManager* in two different scenarios: either for data transformation from a national language to the epSOS Reference Terminology or for data transformation from the epSOS Reference Terminology to a national language).

### 3.2.6 TerminologyServicesAccessManager

This component is called by *TransformationManager*. The component is responsible for translating a given concept designation into the requested target language as well as transcoding a given “local” coded concept into the appropriate epSOS coded concept using the information present in the Terminology Repository. The Terminology Repository is a database that is a part of the NCP and represents the epSOS Reference Terminology. The content of the Terminology Repository is specific for each MS. It is the responsibility of the MS to maintain and update the content of the Terminology Repository.

### 3.2.7 AuditTrailWriter

As required by WP 3.3 WP 3.4, WP 3.6 and WP 3.7 every transaction in epSOS must be audited with very limited information. National requirements for an extended auditing must be realized in the *NationalConnector* or the national infrastructure.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

In future versions it may be an option to start the auditing in an asynchronous manner. For the current version this option will be neglected due to simplicity. Note, that it should be differentiated between logging and audit. Audit captures business-level events (e.g., request for PS) while logging occurs on a lower level and is responsible for capturing application-level events.

### 3.2.8 AuditRepository

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

### 3.2.9 RoutingManager

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

### 3.2.10 ConfigurationAndMonitoringManager

The *ConfigurationAndMonitoringManager* provides a monitoring console that is used for managing configurations of the nation-specific components as well as monitoring their status.

### 3.2.11 NationalConnector

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

## 3.3 EpSOS Front-End Services Transactions

This section describes the end2end interactions between the components of the NCP that correspond to invocations of the epSOS front-end services and that are defined in D3.3.2:


- epSOS Patient Identification Service
- epSOS Patient Service
- epSOS Order Service
- epSOS Dispensation Service
- epSOS Consent Service

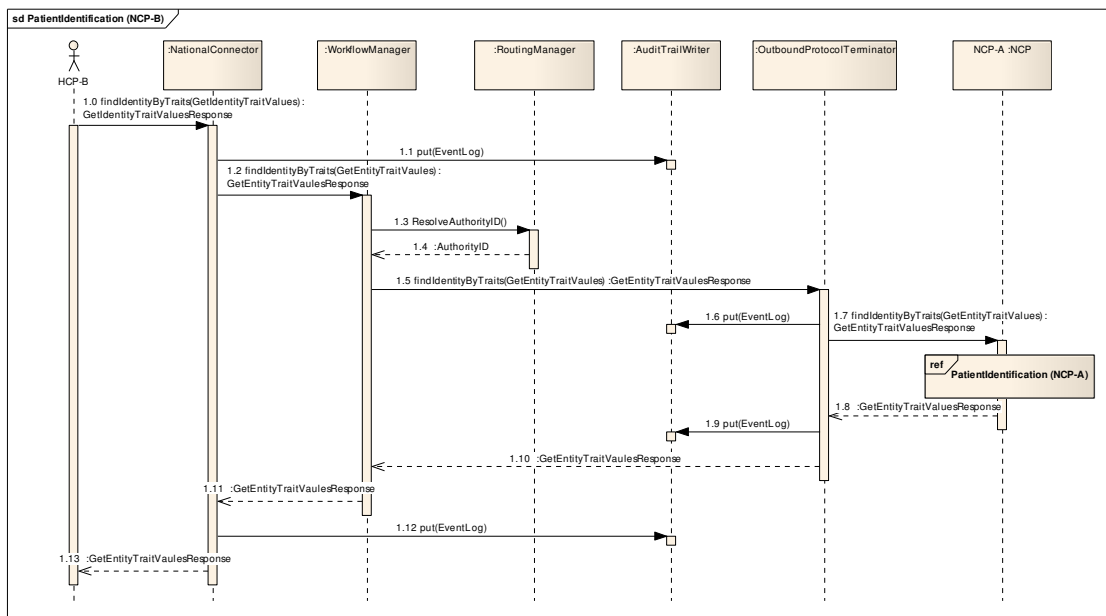
The sequence diagrams provided below shows in which order and by which method calls the NCP components are invoked when one of the front-end services is called.

### 3.3.1 epSOS Patient Identification Service

There are different alternatives to discover a Patient ID and therefore different attributes to be used by calling NCP-B. But all of them result in providing NCP-A with a PID (Patient Identity).


The transaction is visualized by sequence diagrams displayed at Figure 3 and Figure 4:

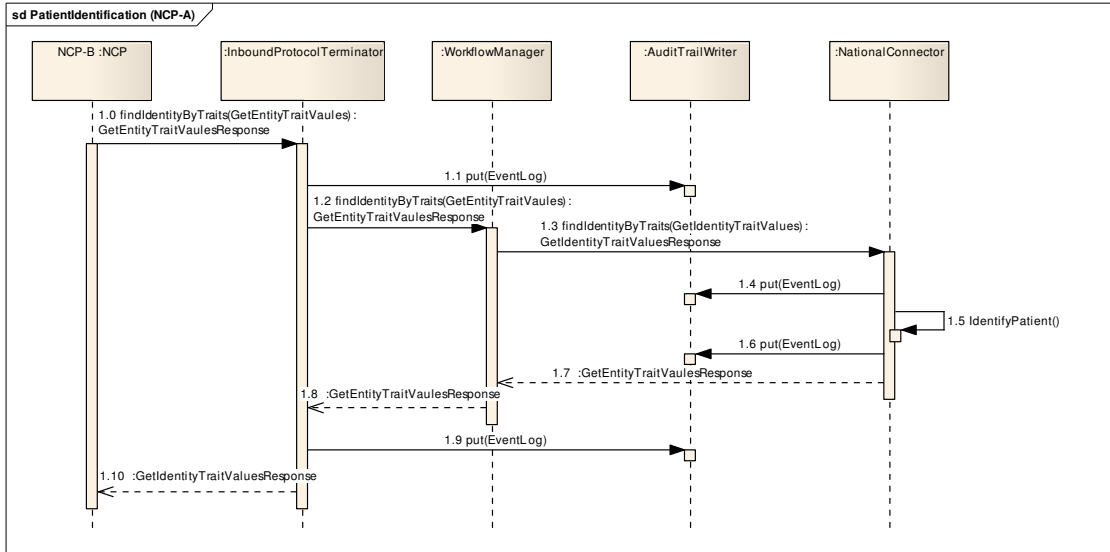
	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010



**Figure 3 Patient Identification - NCP-B**

- [1.0] The HCP in MS B issues a request to the NCP-B by calling an appropriate method of the *NationalConnector* and providing corresponding identity traits.
- [1.1]-[1.2] The *NationalConnector* calls the *AuditTrailManager* to log the patient identification request in the audit trail and forwards the request to the *WorkflowManager*.
- [1.3]-[1.4] The *WorkflowManager* contacts the *ServiceRoutingManager* in order to obtain the URL of the corresponding NCP-A. The URL of the NCP-A is returned.
- [1.5] The request is forwarded to the *OutboundProtocolTerminator*.
- [1.6]-[1.7] The *OutboundProtocolTerminator* logs the patient identification request in the audit trail, wraps the request in a SOAP envelope and issues the SOAP request by performing a remote call of the NCP-A's *IdentityService::findIdentityByTraits()* operation.
- [1.8]-[1.13] As the response it expects a SOAP message containing *GetEntityTraitValuesResponse* with a *PatientID* or status information in case the identification was not successful. Upon a successful identification, the *PatientID* is returned to the HCP with corresponding records made in the audit trail.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010




**Figure 4 Patient Identification - NCP-A**

- [1.0]-[1.1] Upon the arrival of an *IdentityService::findIdentityByTraits()* SOAP request, the *InboundProtocolTerminator* calls the *AuditTrailManager* to log the patient identification request in the audit trail.
- [1.2] The *InboundProtocolTerminator* forwards the trait values to the *WorkflowManager*.
- [1.3] The *WorkflowManager* forwards the identity traits the *NationalController*.
- [1.4]-[1.5] The *NationalConnector* makes a corresponding record in the audit trail and issues a request to the national infrastructure. The response should contain either the ID of the patient (*PatientID*) or status information in case the identification was not successful.
- [1.6]-[1.10] If the identification was successful, the *PatientID* is returned to the *InboundProtocolTerminator* with corresponding records being made in the audit trail. The *InboundProtocolTerminator* wraps the *PID* into a SOAP envelope and sends it to NCP-B as a SOAP response.

### 3.3.2 epSOS Patient Service

The transaction is visualized by sequence diagrams displayed at Figure 5 and Figure 6:

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

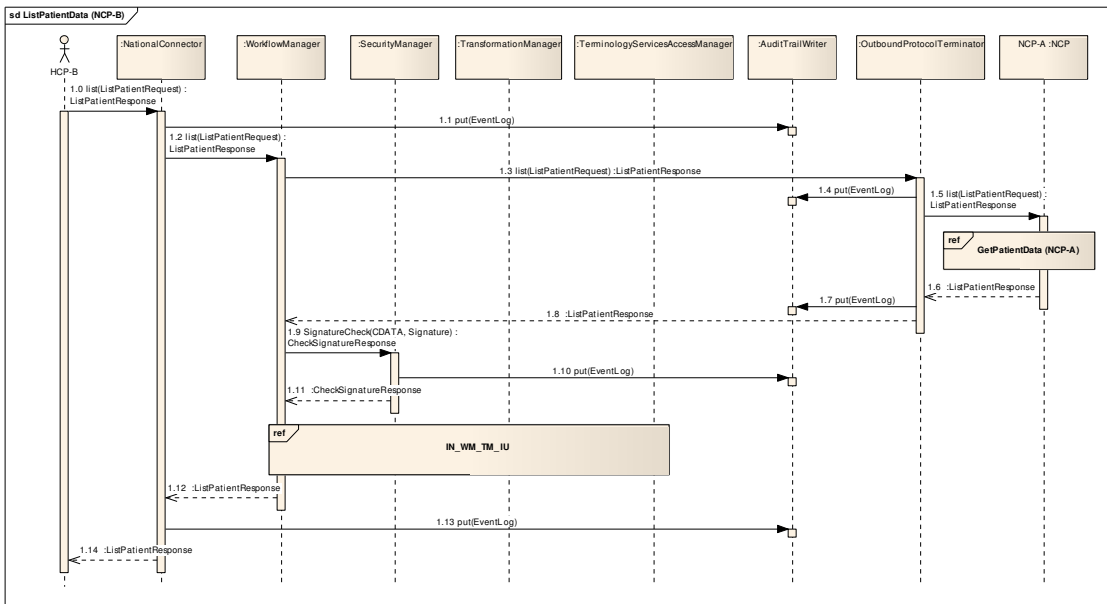

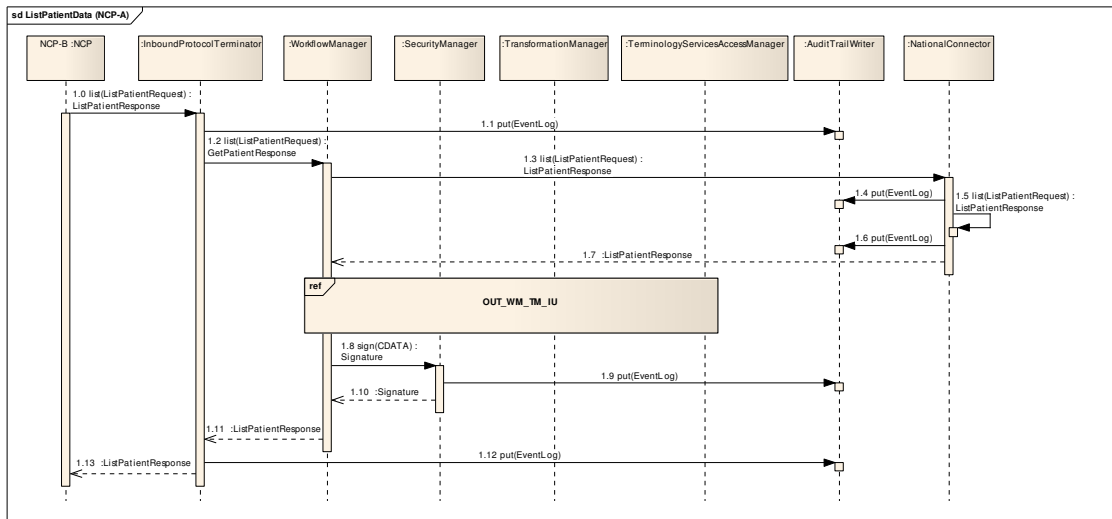


Figure 5 List patient data NCP-B (see Figure 42 for full IN\_WM\_TM\_IU diagram)


- [1.0] The HCP in MS B issues a request for retrieving a PS to the NCP-B by calling a corresponding method of the *NationalConnector* and providing ID of the corresponding patient.
- [1.1]-[1.2] The *NationalConnector* calls the *AuditTrailManager* to log the patient data request in the audit trail and forwards the request to *WorkflowManager*.
- [1.3] The *WorkflowManager* forwards the request to the *OutboundProtocolTerminator*.
- [1.4]-[1.5] The *OutboundProtocolTerminator* wraps the request in a SOAP envelope, logs the request for patient data in the audit trail and performs a remote call of *NCP-A's PatientService::list()* operation by issuing a SOAP request. As the response it expects a SOAP message that contains the patient summary in the epSOS pivot format.
- [1.6]-[1.8] After the PS is found, the *NationalConnector* makes the corresponding record in the audit trail and returns the result to the *WorkflowManager*.
- [1.9]-[1.11] The *WorkflowManager* calls *SecurityService::SignatureCheck()* to verify the signature of the PS. The corresponding record is made in the audit trail.
- [IN\_WM\_TM\_IU] The PS is forwarded to the *TransformationManager* where it is transformed and translated into MS B format.
- [1.12]-[1.14] The translated and signed patient summary is returned to HCP with corresponding records being made in the audit trail.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010



**Figure 6 List patient data NCP-A (see Figure 43 for full OUT\_WM\_TM\_IU diagram)**

- [1.0]-[1.2] Upon the arrival of a *PatientService::list()* SOAP request, the *InboundProtocolTerminator* calls the *AuditTrailManager* to log the patient data request in the audit trail, and forwards the resulting request to the *WorkflowManager*.
- [1.3] The *WorkflowManager* calls *OrderInboundNational::list()* method of the *NationalConnector*.
- [1.4]-[1.5] The *NationalConnector* makes an appropriate record in the audit trail and issues a corresponding request to the national infrastructure. The response should contain the requested PS in the national format of MS A.
- [1.6]-[1.7] After the requested PS is found, the *NationalConnector* makes an appropriate record in the audit trail and returns the result to the *WorkflowManager*.
- [OUT\_WM\_TM\_IU] The successfully verified PS (in MS A format) is forwarded to the *TransformationManager* where it is transformed into epSOS pivot format.
- [1.9]-[1.10] The *WorkflowManager* calls *SecurityService::Sign()* to sign the transformed PS with the NCP-A signature. The corresponding record is made in the audit trail.
- [1.11]-[1.13] The signed PS in epSOS pivot format is returned to the *InboundProtocolTerminator* with corresponding records being made in the audit trail. *InboundProtocolTerminator* wraps the PS into a SOAP envelope and sends it to NCP-B as a SOAP response.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

### 3.3.3 EpSOS Order Service

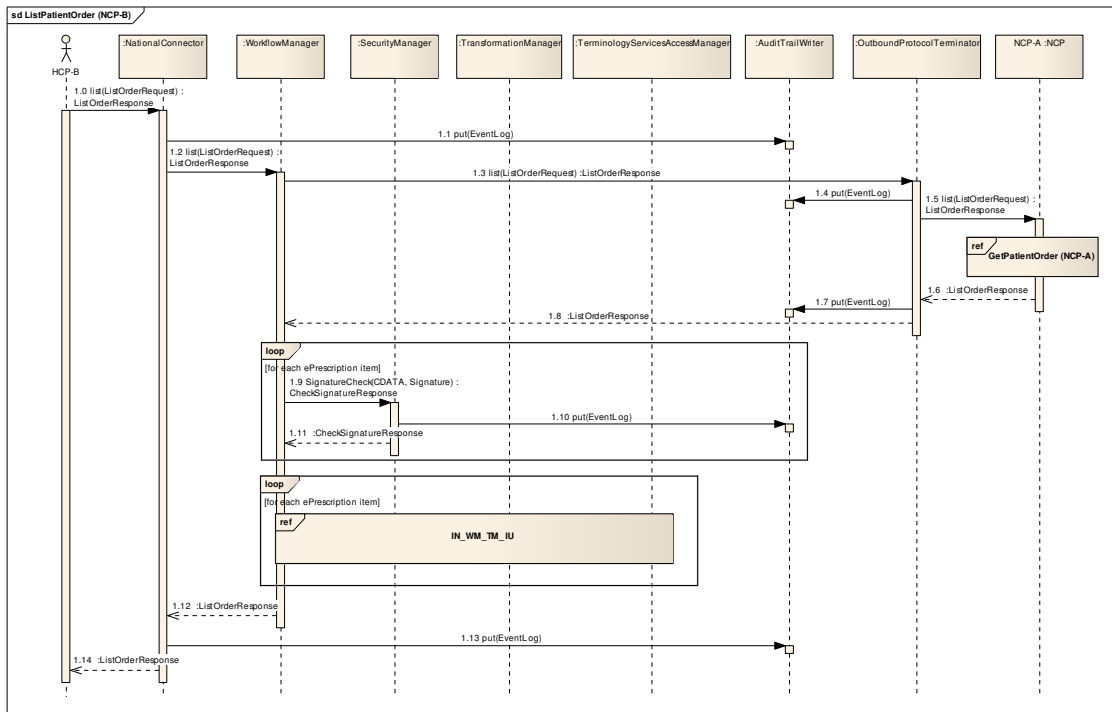



Figure 7 List patient prescriptions NCP-B (see Figure 42 for full IN\_WM\_TM\_IU diagram)

- [1.0] The HCP in MS B issues a request for patient prescriptions to the NCP-B by calling a corresponding method of the *NationalConnector* and providing ID of the patient.
- [1.1]-[1.2] The *NationalConnector* calls the *AuditTrailManager* to log the request for patient prescriptions in the audit trail and forwards the request to the *WorkflowManager*.
- [1.3] The *WorkflowManager* forwards the request to the *OutboundProtocolTerminator*.
- [1.4]-[1.5] The *OutboundProtocolTerminator* wraps the request in a SOAP envelope, logs the request for patient prescriptions in the audit trail and by performs a remote call of *NCP-A*'s *OrderService::list()* operation by issuing a SOAP request. As the response it expects a SOAP message that includes the prescriptions in the epSOS pivot format.
- [1.6]-[1.8] Upon the arrival of the SOAP response, the *OutboundProtocolTerminator* makes a corresponding record in the audit trail, extracts *ListOrderResponse* object from the SOAP response and forwards it to the *WorkflowManager*.
- [1.9]-[1.11] By consequently calling *SecurityService::SignatureCheck()*, the signatures of the arrived prescriptions are verified. The corresponding records are made in the audit trail.
- [IN\_WM\_TM\_IU] The received prescriptions in epSOS pivot format are consequently forwarded to the *TransformationManager* where they are transformed and translated into MS B format.



	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

- [1.12]-[1.14] The translated and signed prescriptions are returned to HCP with corresponding records being made in the audit trail.

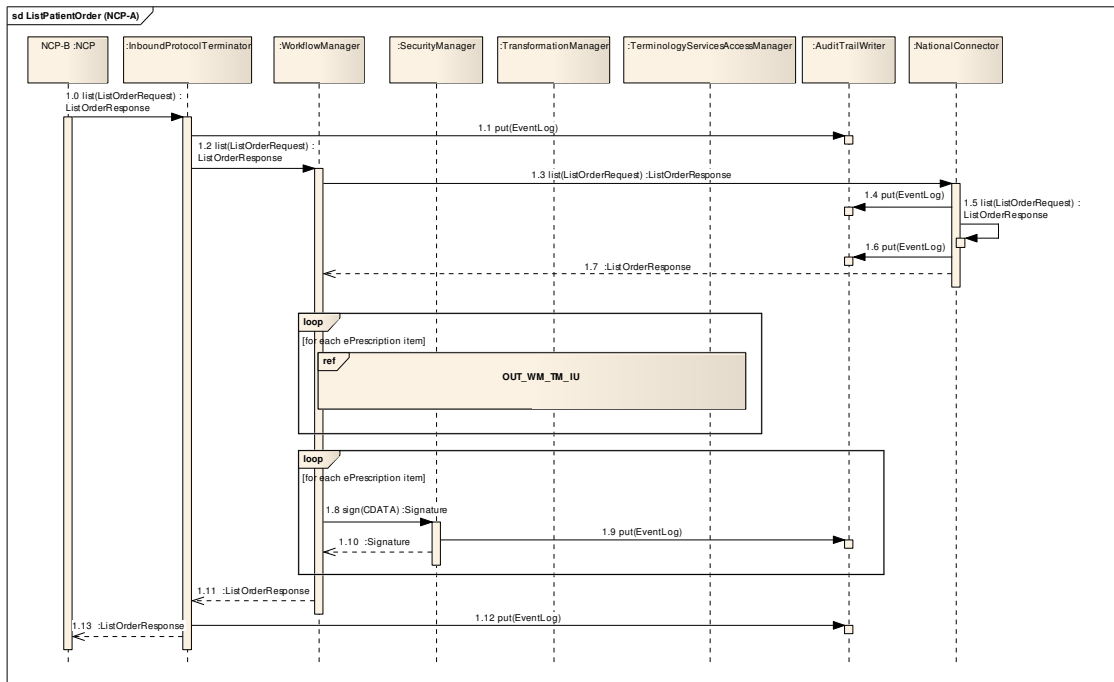



Figure 8 List patient prescriptions NCP-A (see Figure 43 for full OUT\_WM\_TM\_IU diagram)

- [1.0]-[1.2] Upon the arrival of a *OrderService::list()* SOAP request, the *InboundProtocolTerminator* calls the *AuditTrailManager* to log the request for the patient prescriptions in the audit trail, and forwards the request to *WorkflowManager*.
- [1.3] The *WorkflowManager* calls *PatientInboundNational::list()* method of the *NationalConnector*.
- [1.4]-[1.5] The *NationalConnector* makes an appropriate record in the audit trail and forwards the request to the national infrastructure. The response should contain requested prescriptions in the national format of MS A.
- [1.6]-[1.7] After the corresponding Prescriptions are found, the *NationalConnector* makes an appropriate record in the audit trail and returns the result to the *WorkflowManager*.
- [OUT\_WM\_TM\_IU] The successfully verified prescriptions (in MS A format) are consequently forwarded to *TransformationManager* where they are transformed into epSOS pivot format.
- [1.8]-[1.10] By consequently calling *SecurityService::Sign()*, the transformed prescriptions are signed with the NCP-A signature. The corresponding records are made in the audit trail.
- [1.11]-[1.13] The signed prescriptions in epSOS pivot are returned to the *InboundProtocolTerminator* with corresponding records being made in the audit trail. The *InboundProtocolTerminator* wraps the prescriptions into a SOAP envelope and sends it to NCP-B as a SOAP response.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

### 3.3.4 EpSOS Dispensation Notification Service

EpSOS should enable an HCP to dispense a medication or revoke an already provided dispensation. Here sequence diagrams reflecting corresponding *initialize()* and *discard()* calls of the NCP's Dispensation Service are provided.

#### 3.3.4.1 Initializing a Dispensation

The transaction is visualized by sequence diagrams displayed at Figure 9 and Figure 10:

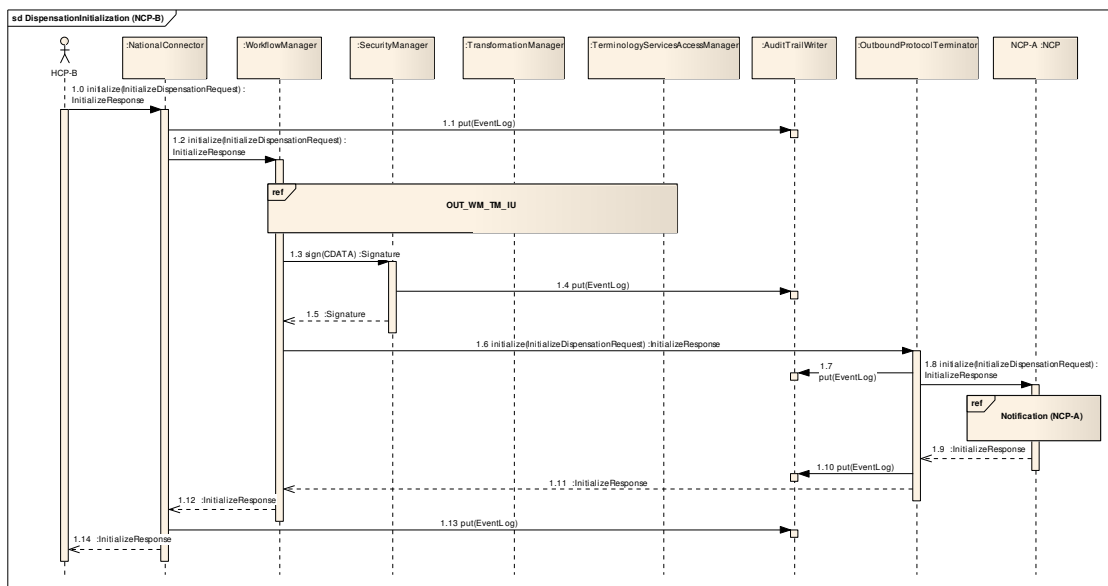

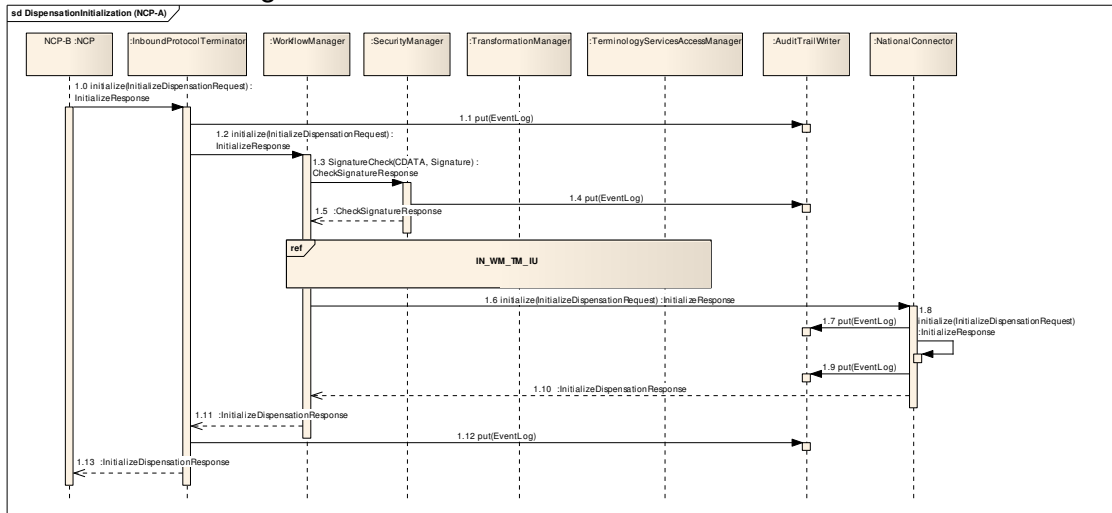


Figure 9 Dispensation initialization NCP-B (see Figure 43 for full OUT\_WM\_TM\_IU diagram)

- [1.0] The HCP in MS B issues a dispensation notification by calling a corresponding method of the *NationalConnector*.
- [1.1]-[1.2] The *NationalConnector* calls the *AuditTrailManager* to log the dispensation request in the audit trail and forwards the request to the *WorkflowManager*.
- [OUT\_WM\_TM\_IU] The successfully verified dispensation (in MS B format) is forwarded to *TransformationManager* where it is transformed into epSOS pivot format.
- [1.3]-[1.5] By calling *SecurityService::Sign()*, the transformed dispensation is signed with the NCP-B signature. The corresponding record is made in the audit trail.
- [1.6] The *WorkflowManager* forwards the transformed in epSOS pivot format and signed dispensation to the *OutboundProtocolTerminator*.
- [1.7]-[1.8] The *OutboundProtocolTerminator* wraps the dispensation in a SOAP envelope, logs the request in the audit trail and performs a remote call of NCP-A's *DispensationService::initialize()* operation by issuing a SOAP request. As a response it expects a SOAP message containing the *InitializeDispensationResponse* that contains the identifier of a defined notification acknowledgement.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

- [1.9]-[1.14] The *InitializeResponse* is returned to HCP with corresponding records being made in the audit trail.




**Figure 10 Dispensation initialization NCP-A** (see Figure 42 for full IN\_WM\_TM\_IU diagram)

- [1.0]-[1.2] Upon the arrival of a *PatientService::initialize()* SOAP request, *InboundProtocolTerminator* calls the *AuditTrailManager* to log the dispensation request in the audit trail, and forwards the resulting object to the *WorkflowManager*.
- [1.3]-[1.5] By calling *SecurityService::SignatureCheck()*, the signature of the arrived dispensation is checked. The corresponding record is made in the audit trail.
- [IN\_WM\_TM\_IU] The successfully verified dispensation in epSOS pivot format is forwarded to the *TransformationManager* where it is transformed and translated into MS A format.
- [1.6] The *WorkflowManager* calls *DispensationInboundNational::initialize()* method of the *NationalConnector*.
- [1.7]-[1.8] The *NationalConnector* makes an appropriate record in the audit trail and issues a corresponding request to the national infrastructure. The response *InitializeResponse* should contain the identifier of a defined notification acknowledgement.
- [1.9]-[1.13] *InitializeDispensationResponse* is returned to the *InboundProtocolTerminator* with corresponding records being made in the audit trail. The *InboundProtocolTerminator* wraps the response into a SOAP envelope and sends it to NCP-B as a SOAP response.

### 3.3.4.2 Discarding a Dispensation

The sequences for discarding a dispensation are identical to the sequences presented on Figure 9 and Figure 10 with *initialize(InitializeDispensationRequest):InitializationResponse* calls substituted by *discard(DiscardDispensationRequest):DiscardResponse* calls.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

### 3.3.5 EpSOS Consent Notification Service

EpSOS should enable a patient to provide or revoke consent for participation in EpSOS use cases while being outside of her country of residence. Here sequence diagrams reflecting corresponding *initialize()* and *discard()* calls of the NCP's Consent Service are provided.

#### 3.3.5.1 Providing a Consent

The transaction is visualized by sequence diagrams displayed at Figure 11 and Figure 12:

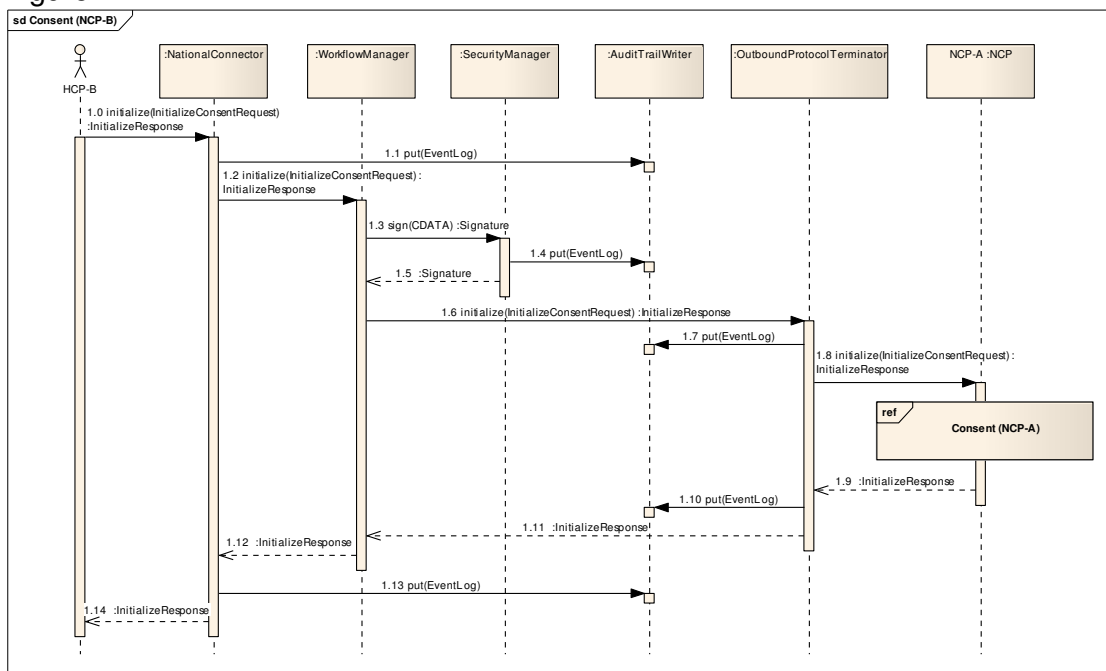

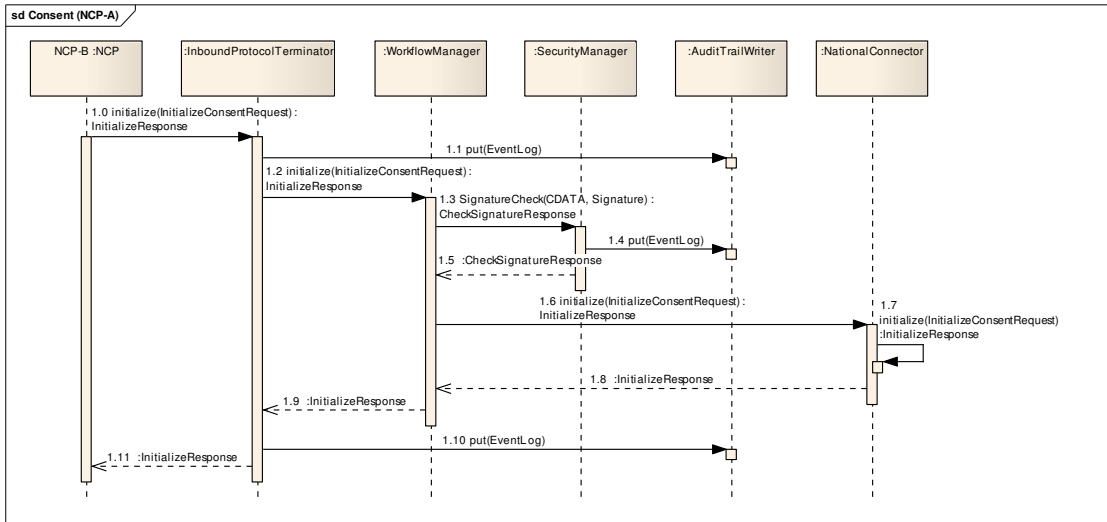


Figure 11 Consent initialization NCP-B

- [1.0] The patient uses the HCP in MS B as an intermediary for providing a consent by calling a corresponding method of the *NationalConnector*.
- [1.1]-[1.2] The *NationalConnector* calls the *AuditTrailManager* to log the consent initialization in the audit trail and forwards the request to the *WorkflowManager*.
- [1.3]-[1.5] By calling *SecurityService::Sign()*, the consent is signed with the NCP-B signature. The corresponding record is made in the audit trail.
- [1.6] The *WorkflowManager* forwards the signed consent to the *OutboundProtocolTerminator*.
- [1.7]-[1.8] The *OutboundProtocolTerminator* wraps the consent in a SOAP envelope, logs the request in the audit trail and performs a remote call of NCP-A's *ConsentService::initialize()* operation by issuing a SOAP request. As a response it expects a SOAP message containing the *InitializeResponse* that contains the identifier of a defined notification acknowledgement.
- [1.9]-[1.14] The *InitializeResponse* is returned to HCP with corresponding records being made in the audit trail.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010



**Figure 12 Consent initialization (NCP-A)**

- [1.0]-[1.2] Upon the arrival of a *PatientService::initialize()* SOAP request, *InboundProtocolTerminator* calls the *AuditTrailManager* to log the consent initialization request in the audit trail, and forwards the resulting object to the *WorkflowManager*.
- [1.3]-[1.5] By calling *SecurityService::SignatureCheck()*, the the signature of the consent initialization is verified. The corresponding record is made in the audit trail.
- [1.6] The *WorkflowManager* calls *DispensationInboundNational::initialize()* method of the *NationalConnector*.
- [1.7]-[1.11] The *NationalConnector* makes an appropriate record in the audit trail and issues a corresponding request to the national infrastructure. The response *InitializeResponse* should contain the identifier of a defined notification acknowledgement.
- [1.12]-[1.16] *InitializeResponse* is returned to the *InboundProtocolTerminator* with corresponding records being made in the audit trail. The *InboundProtocolTerminator* wraps the response into a SOAP envelope and sends it to NCP-B as a SOAP response.

### 3.3.5.2 Revoking a Consent


The sequences for revoking a consent are identical to the sequences presented on Figure 11 and Figure 12 with:

*initialize(InitializeConsentRequest):InitializationResponse* calls substituted by *discard(DiscardConsentRequest):DiscardResponse* calls.

## 3.4 Nation-Specific NCP Components

Every NCP gateway may be Nation-Specific. The term “Nation-Specific NCP Components” in this document is used to identify the components of the NCP that will not be developed in common but are still part of the NCP.


As the NCP Connector connects the national infrastructure to the common components of the NCP it has to implement a defined and stable interface. While

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

the interface must be common the implementation can vary according to the needs of the national systems. If the national infrastructure is based on a messaging system, which is the case in at least some MS, the National Connector will contain components that are similar to the common ones and the following suggestions can be made. It is likely there will be the need of components that encapsulate functionality as described as follows:

- It is suggested to have MSs re-using commonly developed components responsible for the SOAP termination. This will help to ensure interoperability of the NCPs.
- Security services: Dependent on the national implementation of system security and data protection this component may be a subcomponent of the protocol termination. Assuming that certificates are used to provide confidentiality, authenticity and integrity of data this component is for example responsible to validate certificates according to the national policies.
- Message Adaptation: If a tight integration with the national systems is planned it may occur that the message sequences on the national side do not directly map to the corresponding epSOS sequences. For example it may be that certain information in the national infrastructure is transmitted in split messages while in epSOS only one message is used. Another example is that information is distributed and must be consolidated. If that is the case a component is needed which manages the mapping of the message sequences.
- Localization of medical data: the NCP will have to support a nation-specific architecture that implements localization and storage of medical documents.
- Auditing: There will be in any case the need to design and build a component which provides functionality to read audit logs according to the national requirements and legislation. In addition there may be special requirements on the national side which produce the need for an extended auditing.
- Access control: Parts of this feature may be placed in the national infrastructure but there will be the need of a dedicated component in the national connector. At least the stored consent must be read, interpreted and used for the decision making. A structured approach for the component dedicated to access decision control has proved itself as beneficial. Thereby the component is composed of the following subcomponents:
  - The AEF (Access-Control-Enforcement – Facility) controls every data access and thereby makes sure that no access is possible without a former authorization check.
  - The ADF (Access-Control-Decision-Facility) is responsible to provide the decision whether access is granted or not. It makes a decision based on the ADI (Access Decision Information).

Dependant on the architecture and design of the national infrastructure there may be more components needed e.g. for identification of patients or HCPs but the denominated are the most likely.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

### 3.5 Central Common Services Components

According to the conclusions of the joint working group there will be no technical central service providing functionality to the MS (member states). To achieve interoperability between the NCPs centrally managed processes to maintain, update and distribute configuration data is needed.

These processes are to be defined in D3.8.1 and D3.8.2.

### 3.6 NCP-B Internet Front-end

The NCP-B Front End will provide a simple interface for retrieving Patient Summaries (PS), ePrescriptions (eP) as well as for issuing eDispensations (eD). The existence of such a front-end can significantly reduce efforts related to piloting of country B epSOS use cases. For country A uses cases no front end can be used since in this case the NCP-gateway has to be integrated with the national infrastructure.


#### 3.6.1 System Overview

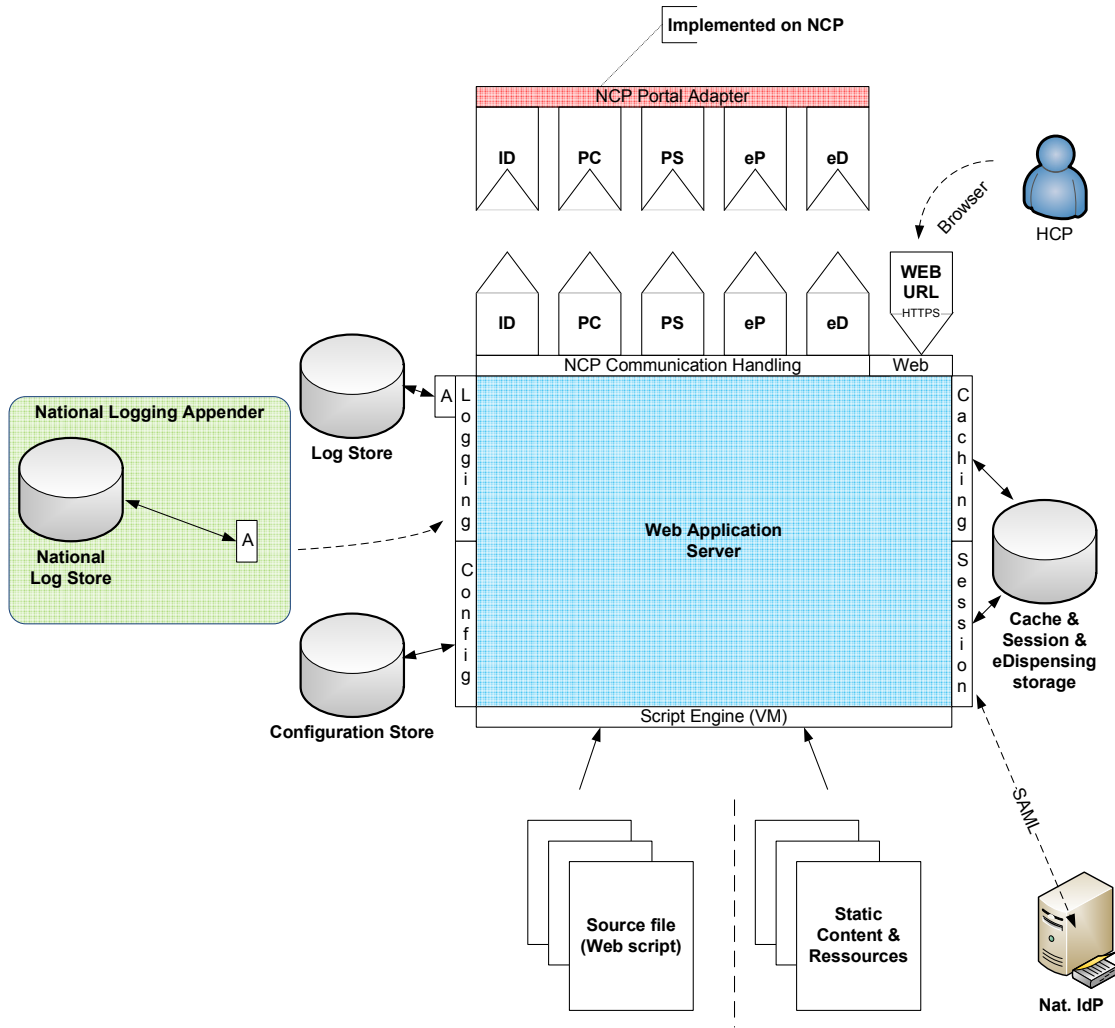
The NCP-B Front-End MUST be build on a Web Application Server/framework, which should be easily to maintain and minimizes development cost & complexity. It SHOULD be based on the enterprise java (Java EE) referable reduced version containing the necessary part for JSP/JSF execution (recommendation), but this can be change with justification. It MUST support the web-services Patient Identification (ID), Patient Consent (PC), patient Summary (PS), ePrescription (eP) and eDispensing (eD); consuming the first four and publishing/sending/pushing the latter.

The interface with/to the NCP MUST go through the NCP Portal Adapter, that decouples the country-B web portal and the core NCP (by this NCP and portal can be deployed in different security zones and multiple, user-group specific portals can be connected to a single NCP). Communication to and from the Front-End to NCP need the Portal Adapter, because the National Connector is unknown (national specific), and therefore to have a common/unique interface between the two systems, a portal specific adapter is needed.

The connectivity between the NCP Portal Adapter and the NCP-B Front-End can be java-to-java technology, Plain Old Java Object (POJO), but it MUST be so, that the Front-End and the Portal adapter can be separated by network zone and physical execution environment. The transportation of POJOs can easily be facilitated with the Spring Remoting framework or equivalent.

The System overview below is informative.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010	




**Figure 13 Front-End System Overview**

The frameworks/products etc. to-be used in the Front-End development SHOULD be chosen according to the NCP Implementation Platform description.


The System overview above shows that a *national* logging Appender (marked with 'A') can be made, so that logging is performed, also on a national logging system. A common well-tested framework for logging with Appender (marked with 'A') setup is Log4j (recommended). Log4J supports addition/special appenders for auditing to special sources (national). Furthermore it supports auditing/logging to multiple sources, there another chosen framework, than Log4J, SHOULD support the same functionality (justification).

The standard implementation needs storage of log, configuration, cache, sessions & eDispensing rapports information (shown with dB-symbols). Furthermore source files (enterprise java ~ Java EE) must be accessed along with static content/resources at Web Application start-up.



	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

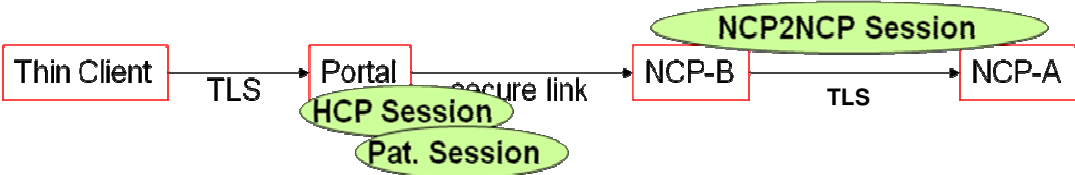
Front-end component	Description
Web Application Server	Web- and/or application Server to execute the NCP Front-end B application
Script Engine	Environment for compiling, executing Web Script files and needed resources etc.
Configuration Store	Storage needed by the configuration framework of the Front-end application
Log Store	Storage needed by the logging framework of the Front-end application
National Logging Appender	A logging appender (module / component), which is not part of the Front-end delivery, but shall be a possibility for MS implementers. The appender can write logging/audit entries to the national logging/audit store (standard feature in Log4J).
Cache, Session & eDispensing store	Database Storage for storing cache information, HCP& Patient sessions, as well as eDispensing rapports.
National Identity Provider (IdP)	National system for identifying HCP using SAML 2.0 and SAML WebSSO, not part of Front-end solution, national responsibility.
Web interface	Interface for HCP access to NCP Front-end B portal, uses HTTP-over-SSL (HTTPS)
NCP communication handling	Interface to the NCP based on POJO interface by communicating Java object over-the-wire.
Portal Adapter	Adapter located in the NCP for enabling the communication between the NCP and Front-end without using the unknown National Adapters. This adapter is part of the NCP, and therefore not the Front-end.
ID	Transaction needed for enabling patient identification (NCP is provider, Front-end is consumer)
PC	Transaction needed for enabling Patient

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

	Consent documents (NCP is provider, Front-end is consumer)
PS	Transaction needed for enabling Patient Summary documents (NCP is provider, Front-end is consumer)
eP	Transaction needed for enabling ePrescription documents (NCP is provider, Front-end is consumer)
eD	Transaction needed for enabling eDispensing documents (NCP is provider, Front-end is consumer)

### 3.6.2 Security


The web application MUST when ever sessions are used, use Server-Side session, which are invisible to the client. Furthermore the application SHOULD use standard web-server security measures.

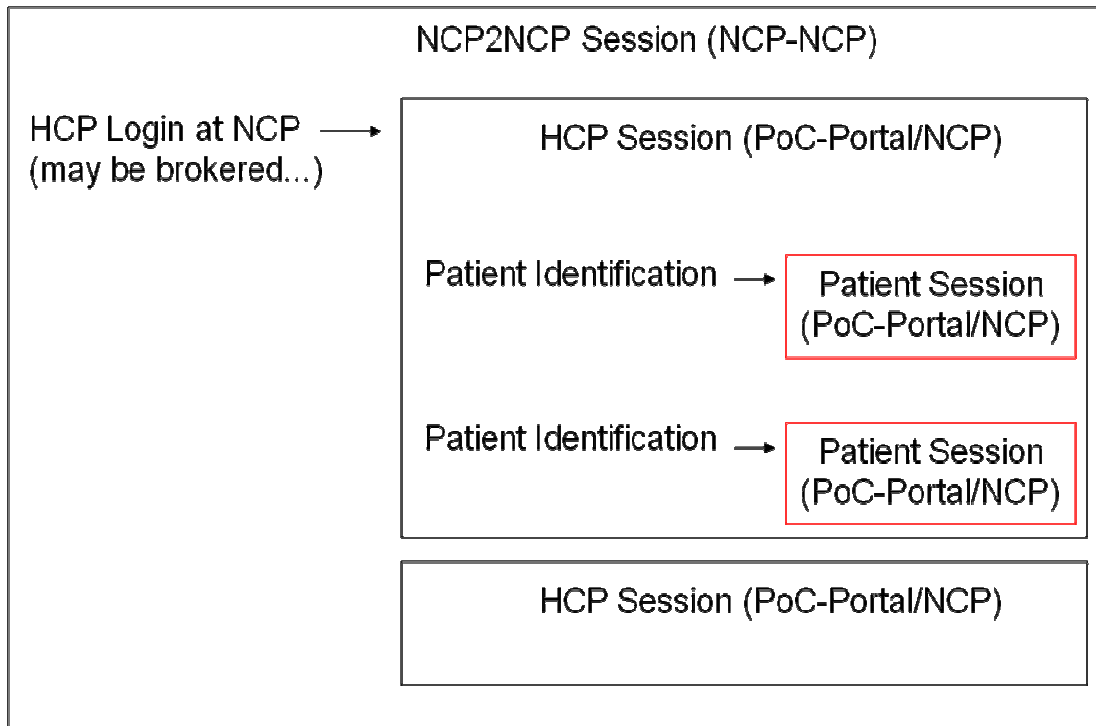


**Figure 14 Security of Front-End solution (portal)**

The user browser access to the portal MUST be only acceptable by HTTPS/TLS with at least 128bit encryption. This MUST be implemented with a MS specific certificate which is certifiable (can be checked by national certificate authorization (CA)).

The portal MUST use a secure link to national side of NCP, which MUST be terminated in the NCP Portal Adapter (see Figure 1 (NCP-in-a-transparent-box)).

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010




**Figure 15 Session management in country B**

The session needed for NCP & Front-end implementation according to the epSOS standard are a NCP2NCP session (Mutual Trust), a HCP Session for each HCP Authentication (HCP Confirmation Assertion), which can be brokered via the National IdP & a patient Session for each identified patient (TRC Assertion), which shall not be over-lapping in each HCP session, to provide patient security by isolating patient data.

### 3.6.3 HCP Authentication

HCPs acting as a PoC in a country B shall have the option to use the web portal to access epSOS services. Strictly speaking, this is part of the national infrastructure, but as that part of the NCP is useful to a number of MS, it will be provided as part of the NCP-In-A-Transparent-Box. With respect to Identity Management, the interface will be based on the SAML industry standard, more specifically on the Web-SSO profile. The rationale for that is:

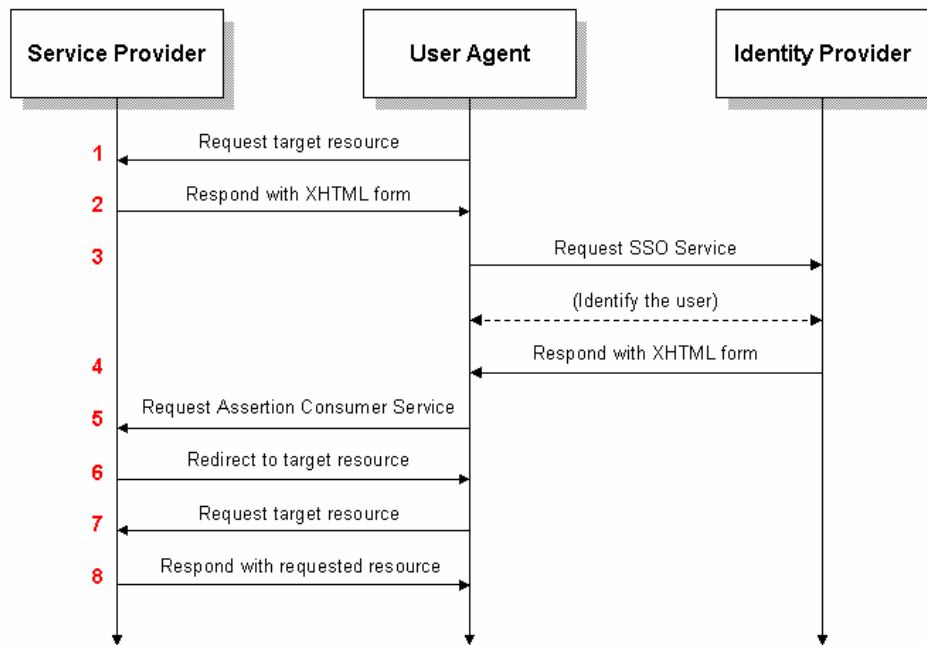
- SAML is the most commonly used standard for the Web-SSO use case, and there are a number of quite well interoperable implementations.
- If there is no existing Identity Provider (IdP) for HCPs in a MS, there are a number of solid open source implementations available, that can be used for operation and NCP development.
- SAML-based IdP's might be used for web service authentication as well with co-existence of browser and WS-base access in a single solution.
- The complexity of various authentication mechanisms is delegated to an IdP external to the NCP

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

The NCP-B Front-End MUST use the SAML 2.0 for standard authentication and assertion.

### 3.6.3.1 Use Case

The Web-SSO use case delegates the management of use authentication, attributes and authorization to one or several Identity Providers. The following constraints shall limit the complexity of implementation and increase interoperability. There might be separate authorities for HCP authentication and HCP attributes (like who is a GP). The use case assumes, that HCP attributes are available to the IdP in a secure way (web service, LDAP over SSL, etc.) and issued by the IdP as SAML attribute assertion.




**Figure 16 SAML Web SSO Sequence Diagram**

The SAML Assertion received from the Identity Provider (IdP) MUST provide the epSOS attributes needed for issuing the HCP Identification SAML assertion.

The flow control is as follows:

1. The User Agent (i. e. Web Browser) calls the Service Provider (i. e. NCP Frontend).
2. The Service Provider responds with a XHTML form containing the localization information of the trusted Identity Provider.
3. The User Agent performs the authentication of the logged in user.
4. The Identity Provider responds with a XHTML form that contains the SAML Assertion.
5. The User Agent calls the Service Provider again, but with the issued assertion.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

6. The Service Provider accepts the SAML Assertion and responds with a redirect to the target resource.
7. The User Agent requests the resource that is provided by the Service Provider.
8. The Service Provider responds with the requested resource.

Mapping of terms in figure 14 to epSOS Front-end terms

SAML WebSSO Term	NCP Front-end equivalent
Service Provider	Front-end – Web Interface
User Agent	HCP Browser for Front-end access
Identity Provider	National Identity Provider (IdP)

### 3.6.3.2NCP Web-Portal SAML profile

- Only SAML 2.0 needs to be supported, SAML 1.1. is not considered
- Authentication is always initiated from the SP; IdP-discovery can be any type.
- Authentication Request with both HTTP Redirect and HTTP-Artifact bindings
- All IdP-SP communication uses HTTP
- Request may be unsigned

Authentication Response:

- Binding HTTP POST
- Assertion must be signed.
- Attributes should be contained in the authentication response in one assertion in a single AttributeStatement .

Attribute Query

- SP Authentication shall support HTTPS (signed requests are optional)

HCP Attributes

- All attributes are available to the IdP as attribute authority, and can be queried by the SP using an SAML query.

Single Logout (SLO)


- SP-initiated SLO must be and IdP-initiated SLO should be supported.
- LogoutRequest and LogoutResponse MUST be signed.
- If Single Logout is unsuccessful, user MUST be informed.

### 3.6.3.3SAML Authentication Context Classes

Initially, X.509 client certificate based authentication is required. IdP and SP MUST ensure that the client is using the same certificate for authentication and resource access. Otherwise, there is no restriction on client authentication mechanisms.

### 3.6.3.4Metadata Distribution

IdP meta data must be signed for operational use.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

### 3.6.4 Site Collection

The NCP-B Front-End site/portal pages SHOULD have the structure shown below, that is the navigation tree is informative, but functionality within SHOULD be present.

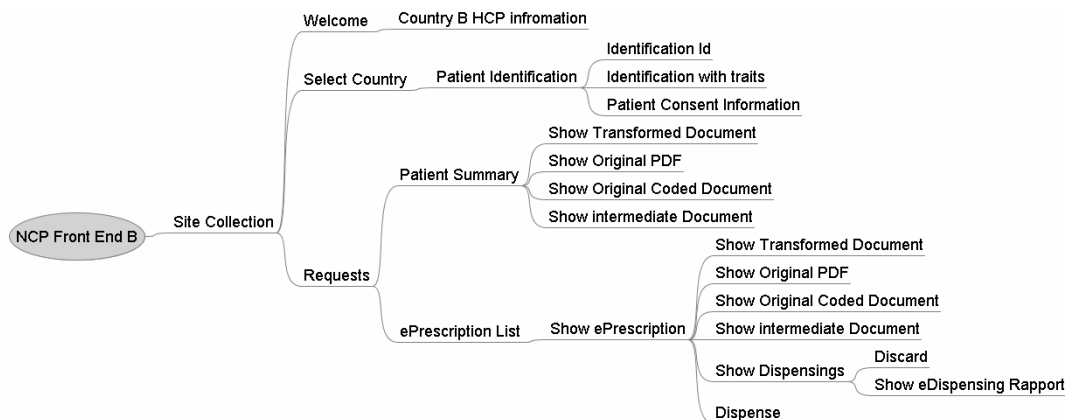



Figure 17 Site diagram (Site Collection)

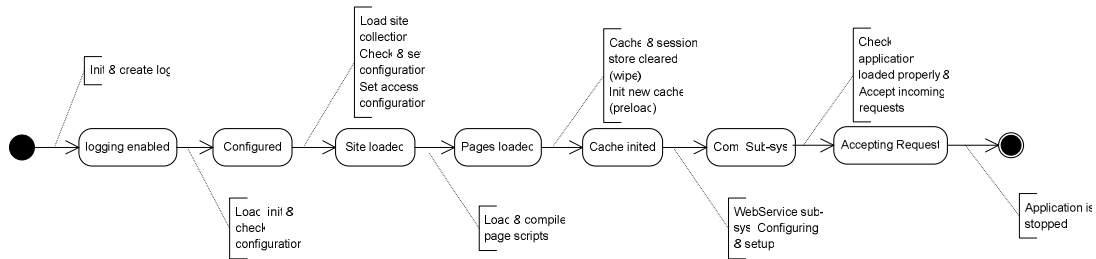
The pages in the site-collection are not listed in detail, but should be self-explanatory with little knowledge with epSOS project; however the clinical information pages are explained in the following table.

Page name/type	Description
Show Transformed Document	Page showing the structured transformed data coming from the Pivot CDA document
Show Original PDF	Page/link to CDA embedded PDF/A document (launch of browser registered PDF viewer)
Show Original Coded Document	Page showing the structured original data coming from the Pivot CDA document. The data is unhampered by the transformation processes in the two communicating NCPs.
Show Intermediate Document	Page showing the structured epSOS intermediate data coming from the Pivot CDA document. The data is in the epSOS coding & epSOS language (English)

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

### 3.6.5 Application Life-Cycle

The NCP-B Front-End application MUST have an application life-cycle, which is checked by the application, so that a controlled start and stop is performed. Each state can only be entered if the previous action was successful. The life-cycle below is informative.

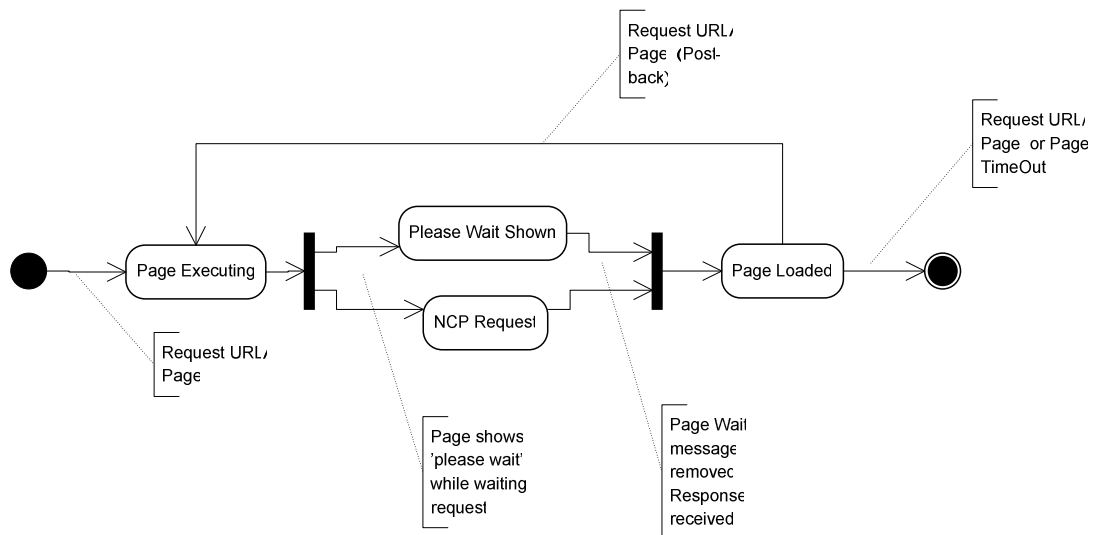


**Figure 18 Application Lifecycle (Informative)**


An important step in above is the clearing/wiping of cache & session stores; to avoid information creep between sessions etc. These are for security normative and MUST be performed before accepting of client requests.

### 3.6.6 Page Life-Cycle

The NCP-B Front-End application MUST have an application/web page life-cycle, which is checked by the application, so that page loading and request/response is controlled. Each state can only be entered if the previous action succeeded. The life-cycle below is normative, showing that Front-End requests to NCP are performed in parallel to page showing a 'Please Wait'-sign. This sort of parallel execution CAN e.g. be performed in AJAX (Client-Side) or Server-Side. This life-cycle start MUST only be accessible from Application life-cycle state: "Accepting Requests"

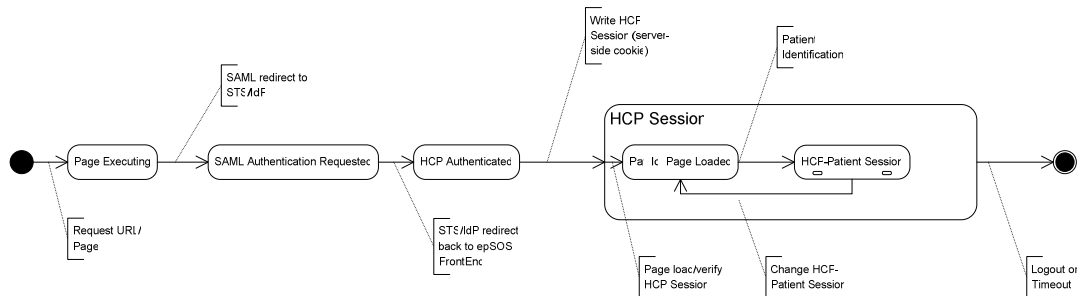


**Figure 19 Page Lifecycle (NCP request handling)**

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

### 3.6.7 HCP Session Life-Cycle

The NCP-B Front-End application MUST have an HCP Session life-cycle, which is checked by the application, so that HCP authentication, access-control & timeouts are controlled. Each state can only be entered if the previous succeeded. The life-cycle below is normative, showing that HCP authentication MUST be done before actual patient identification can be performed. This life-cycle start MUST only be accessible from Application life-cycle state: “Accepting Requests”




**Figure 20 HCP Session Lifecycle**

The HCP Session is store on the Front-end Web Server (Server-side), as a entry/object in a session store for controlling access and state of HCP session.

The authentication MUST be via direct- or brokered trust SAML assertions. This MUST be done using the SAML 2.0 Web Single-Sign-On (SSO) profile. Below this is shown on the right. On the left a deployment is shown, where HCPs directly authenticate with the NCP.



	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

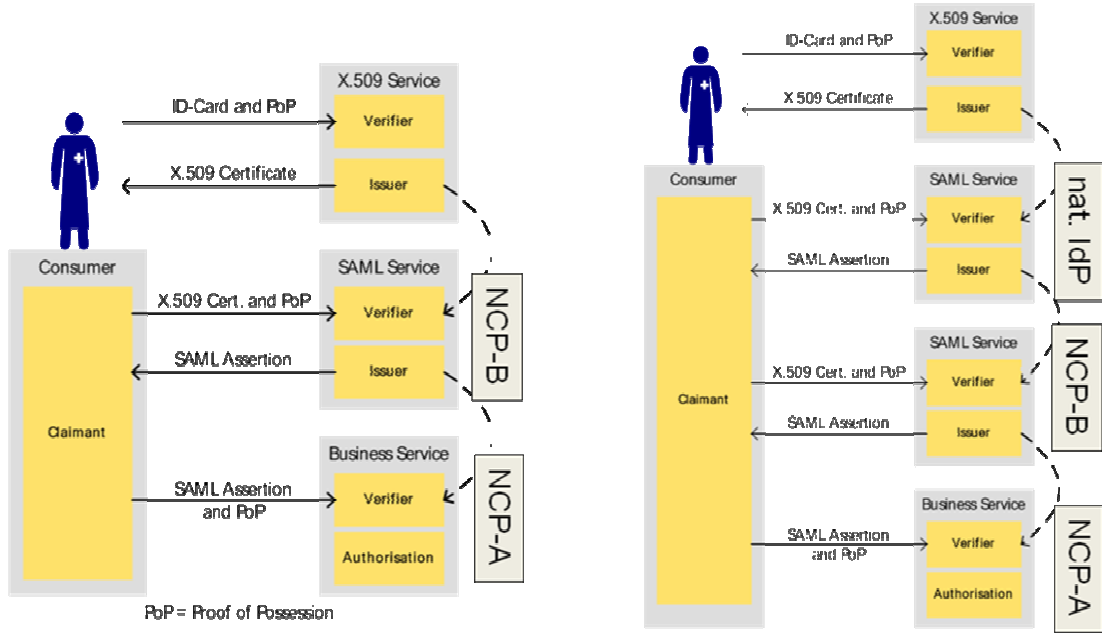



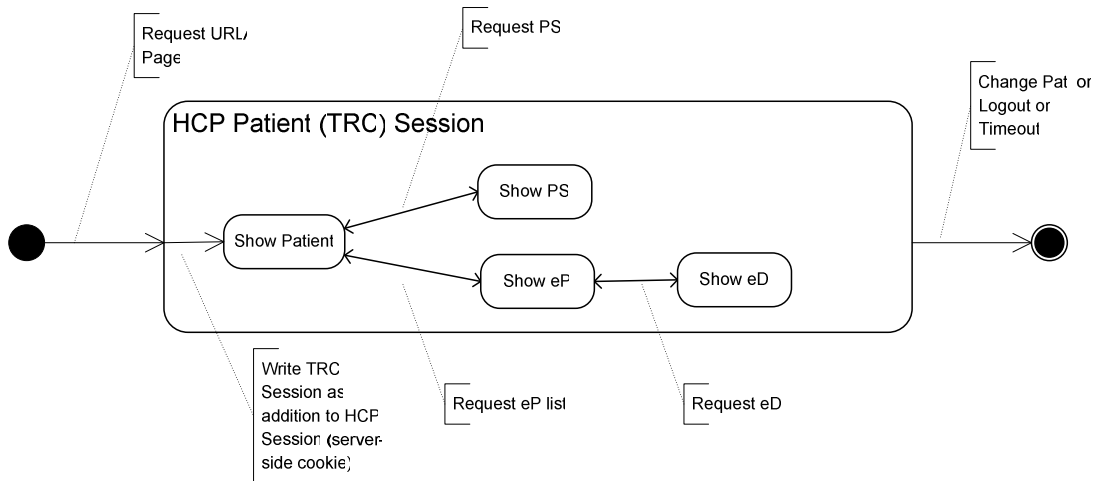
Figure 21 Example from NCP assertion trust

The IDP can only issue identity assertions; The TRC must be issued by the portal.

### 3.6.8 HCP Patient (TRC) Session Life-Cycle

The NCP-B Front-End application MUST have an HCP Patient/Treatment Relationship Confirmation (TRC) Session life-cycle, which is checked by the application, so that an authenticated HCP with an identified patient can access patient data in a controlled manner. Each state can only be entered if the previous action was successful. The life-cycle below is normative, showing that HCP MUST perform patient identification before patient data can be retrieved. This life-cycle start MUST only be accessible from HCP Session life-cycle state: "HCP-Patient Session".

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010



**Figure 22 HCP Patient (TRC) Session Lifecycle**


The handling of multiple session and cascaded session in the Front-end application must be manually implemented if Java environment does not support this, depending on versions hereof.

## 4 Example Deployment Composition

Since all major actors or components inside the NCP-In-A-Transparent-Box are introduced in previous chapters, now a closer look how they might be deployed is given.

Introductory, the figure below depicts the placement of both NCPs. A Thin Client (Browser-based epSOS Portal or Front-end) enforces an authentication via a trusted Authentication Service, i.e. Identity Provider. The protocol used (either SAML Protocol or WS-Trust Protocol) is out of scope for the NCP implementation. Only the outcome of the Identity Provider – the (signed) SAML assertion (Identity Assertion) - issued by a trusted party located in the national infrastructure - is relevant. The epSOS Portal invokes the NCP-B providing all specified epSOS services. The Workflow Manager in NCP-B then sends by using the Outbound Protocol Terminator a cross-border SOAP request to the NCP-A of the patient's home country. This SOAP request is fully compliant to the epSOS D3.4.2 normative request message specification. Then, the NCP-A processes this request by using the common components bundled with the NCP-A. It furthermore uses the services that are located in the national infrastructure. In any case, the NCP-A responds with a message according to the specified D3.4.2 epSOS message format.

Figure 23 shows the proxy semantic of a NCP-B. That is, a generic Java-based invocation message is transformed into the epSOS format and forwarded to another NCP-A, and finally mapped on national specific service requests. For simplicity, only relevant components are shown, those which have an impact on the communication with involved services or other components. The flow of control with regard to the common components of the NCP is given in the next section.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

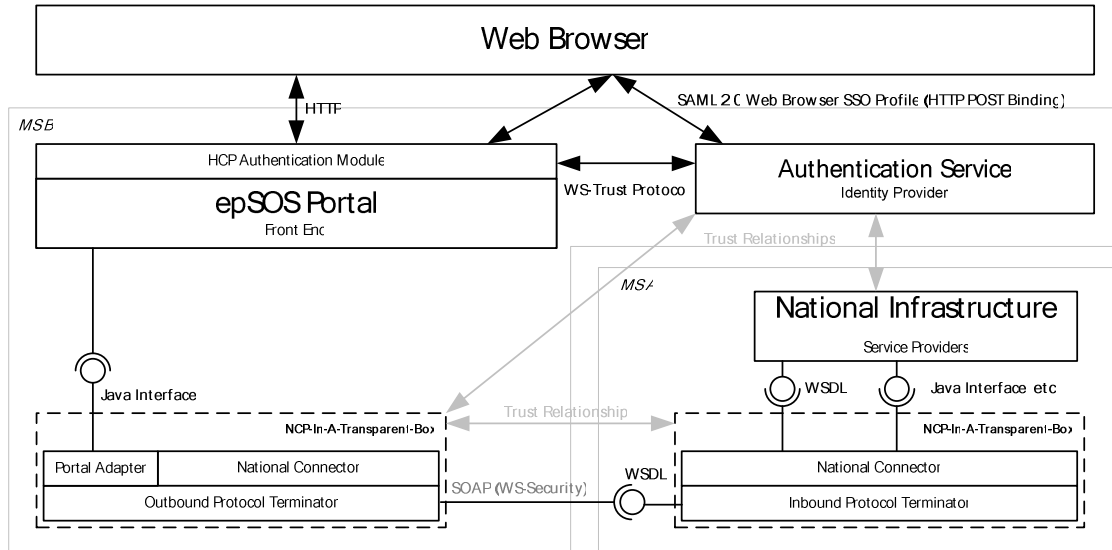


Figure 23 Logical View for both NCPs<sup>2</sup>

## 4.1 Navigation Paths


Since the NCP takes different roles in the Circle of Trust, the navigation paths for the message flow are exemplary shown below. Therefore a NCP provides three interfaces which are also described. These ones are the (1) NCP-B Interface, the (2) NCP-A Interface, and the Central Common Service Interface.

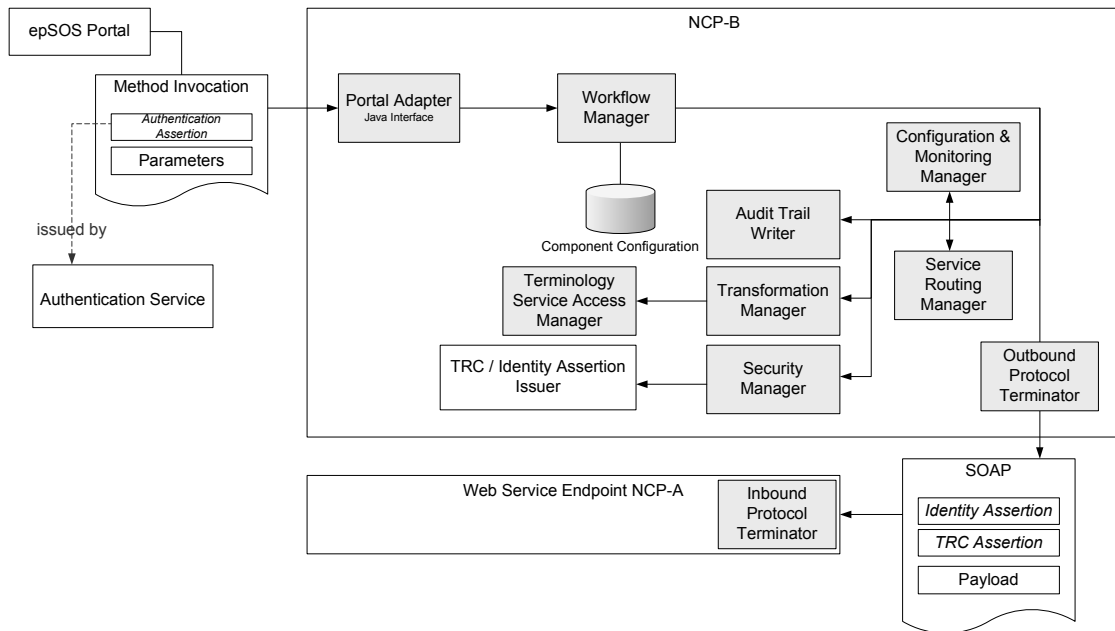
### 4.1.1 NCP-B Role

The epSOS portal invokes a method provided by the portal adapter interface of the National Connector. The portal adapter forwards the request to the Workflow Manager, that makes use of various common components in order to process the request:

- the provided assertions need to be validated, e.g. it has to be checked whether the epSOS profile is used.
  - routing information needs to be obtained from the epSOS NCP configuration
  - audit trail entries need to be written
  - for eDispensations a mapping of the national format and taxonomies to the epSOS format has to be done. For ePrescriptions and patient summaries a mapping from the common epSOS format to the national format and vocabularies has to be done.
- Finally, a SOAP request message is created and sent to the cross-border NCP-A. The response is mapped on the interface of the National Connector so that the epSOS Portal is able to render it accordingly.

<sup>2</sup> This figure shows a sample deployment. E.g. instead of WS Trust the SAML protocol could be used as well for obtaining the HCP identity assertion.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010




**Figure 24 Overview for NCP-In-A-Transparent-Box in NCP-B Role**

The epSOS Front-end is logically separated from the NCP-In-A-Transparent-Box. However, it is tightly bound to it, because the Front-End provides the user interface for the epSOS services which the NCP delivers or supplies. What is solely taken into account when regarding the NCP-B role is the communication between the Front-end and the National Connector that the NCP-B provides. Until now, the interface to be specified is an ordinary Java one, which accepts POJOs (Plain Old Java Object) as parameter values. Further information on the technology that implements the serialization and de-serialization of them is given in section 3.6.1.

#### 4.1.2 NCP-A Role

The incoming SOAP messages are processed by off the shelf Web service frameworks (cp. section 5.21). A registered Web service endpoint listener is called by the framework. Previously, the SOAP message was validated against the policy according to the WSDL document. For instance, this includes the token mapping (i.e. are SAML assertion(s) and signatures present), or the validation of timestamps stated in the message header. SOAP message handlers provide the possibility to access the entire SOAP envelope and might pre-process relevant data. The Endpoint Listener issues synchronous (blocking) requests to the Workflow Manager component. Then, this component uses registered components in order to process the request. In the end, the services located in the national infrastructure are invoked by means of the National Connector in order to create the SOAP response for NCP-B. The following figure sketches the role of a NCP when it is called by another NCP-B.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

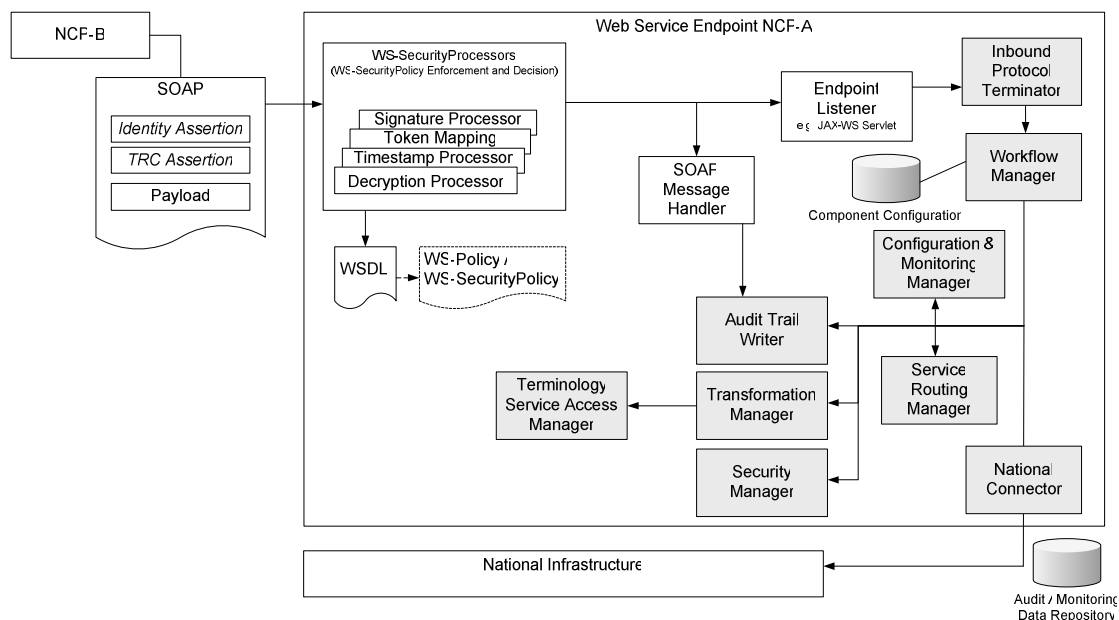


Figure 25 Overview for NCP-In-A-Transparent-Box in NCP-A Role

### 4.1.3 Central Common Service Role


There exist several external services that are consumed by a NCP implementation in order to process a request. In the TPM meeting of February 17(th), 2010 it was decided that the configuration data should be processed using a static document that is shared e.g. in Project Place. Regardless of the origin of the configuration (e.g. document or dedicated services), each NCP has to be initialized and put into operation in a normalized manner. This necessitates that a common interface is available for relying components inside the NCP. Section 3.2.10 introduced the Configuration and Monitoring Manager which encapsulates the source of the configuration. The access to the configuration data needs to be defined subsequently.

## 4.2 Deployment

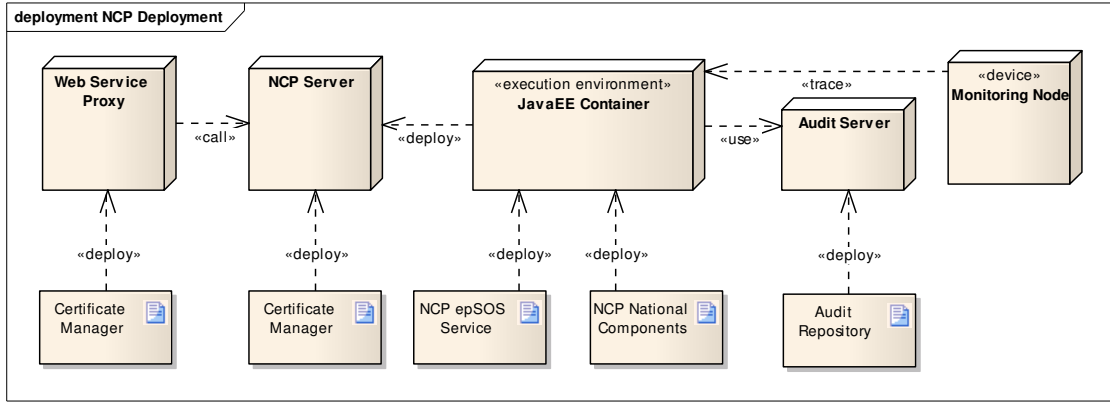
Comments to the deployment diagram:

- Segregation of duties requires that the audit repository and NCP service MUST run in separate administrative domains. This does not require separate physical servers, but safeguards, that the NCP administrative staff does not have access to the audit repository. (D3.7.2 does not propose an epSOS-centralized audit service; the audit repository is still in control of the member state).
- Transport layer security configuration is dependent on whether a web service proxy must be installed. (Opinion: Using a web service proxy makes certificate management more cumbersome, for a very small security advantage.)

There are no specific hooks for monitoring services at the application level; (Except for real-time abuse detection, but that is yet unspecified). The following figure

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

sketches the exemplary deployment of the common components in a NCP and its related services used.



**Figure 26 – Exemplary Deployment of the NCP Components**

### 4.3 Implementation Platform

epSOS Common software will adopt Open Source frameworks and applications as much as possible.


Reference implementations will be made available on a single platform. To open vendors a wide range of options, the only two requirements are:

- RedHat Enterprise Linux
- Java Enterprise Edition

Vendors will have to specify the dependency of their solution on languages, frameworks, APIs and applications; the detailed specification will contain a sample list. All choices of frameworks, libraries application environment must be compatible as specified from source and by vendor test.

The goal of the following table is to provide a first list of software languages, frameworks and applications for epSOS software commonly developed components and for epSOS commonly developed Front-end.

Element	Required	Options / choices / Recommendation
Languages	Java EE	Choice between version 5 or 6
Operating System		RedHat Enterprise Linux (64bit) Choice between version 4 or 5
Application Server		Recommended choice between <ul style="list-style-type: none"> <li>• JBoss v.4 or 5</li> <li>• Glassfish v.3</li> </ul>

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

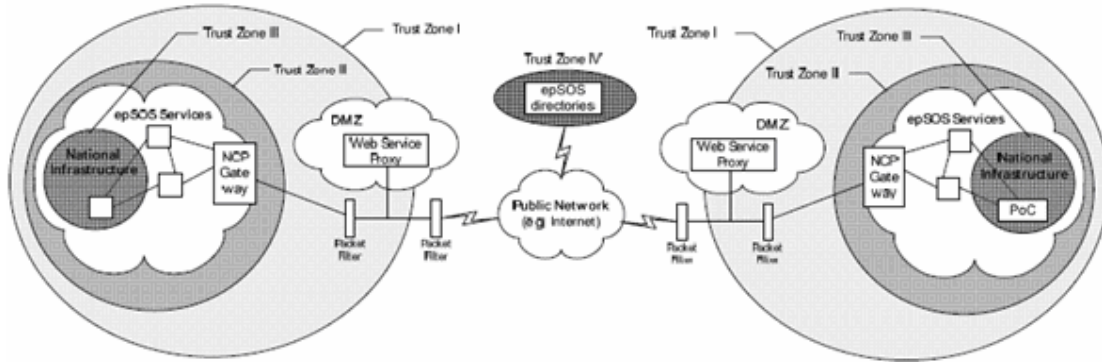
Element	Required	Options / choices / Recommendation
		<ul style="list-style-type: none"> <li>Tomcat v.5.x / 6.x</li> </ul>
<b>GUI</b>		Recommended build upon JSP/JSF
<b>Security SAML Framework</b>		Recommended <ul style="list-style-type: none"> <li>OpenSAML library</li> </ul>
<b>Security WS-* Framework</b>		Choice between <ul style="list-style-type: none"> <li>SUN METRO</li> <li>AXIS2</li> </ul>
<b>Audit Framework</b>		Recommended using log4j for audit logging

## 4.4 Security Setup for NCP

### 4.4.1 Security Zones


This section is informative to the MS, however likewise security mechanisms **MUST** be adopted by the MS in accordance with D3.7.2.

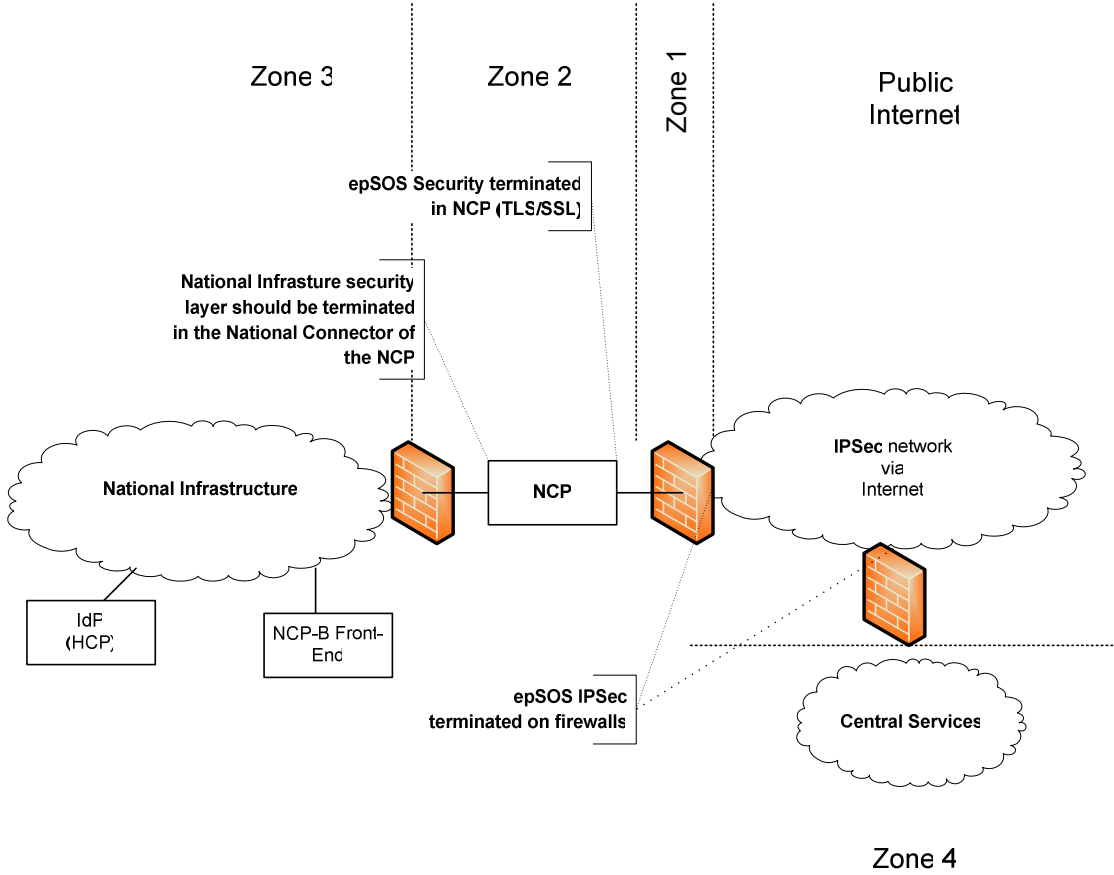
Figure below from D3.7.2 shows the security zones for epSOS setup of the NCP.



**Figure 27 General epSOS Trust Zones**


Adaptation of the security zones to the “NCP in a transparent box” approach, i.e. the NCP is a gateway (box), which is seen as both secure (national) and un-secure (entrance of internet traffic). To strengthen the protection both for the national infrastructure and the traffic entering the epSOS p2p network, the NCP is placed in its own security zone, guarded by two firewalls.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010




System / Zone	Description	Security Mechanisms
epSOS central services	<p>Central Services placed in the epSOS p2p network (Internet), should be guarded by the same security as the NCP zone, since the information is used by NCP.</p> <p>The central services might be implemented as virtual following the p2p paradigm and there would physical be placed in the NCP zone. Virtual central services, are seemingly at a central place, but actually physically at the NCPs (decentralized). Only the reference mechanism is central (referenced by DNS).</p>	Same as NCP gateway and zone.
NCP gateway	NCP gateway in its own zone.	Hardened Platform



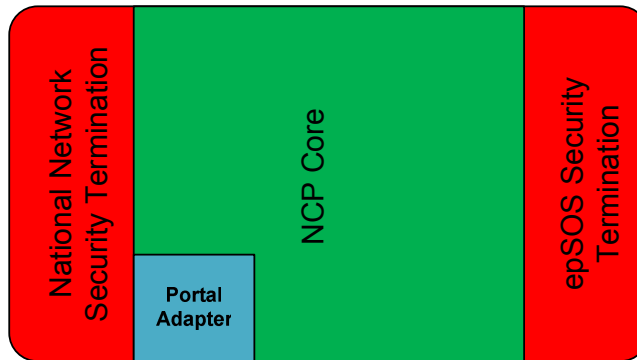
	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

System / Zone	Description	Security Mechanisms
	<p>The NCP MUST terminate the layer 4+ (SSL/TLS) on the NCP gateway platform inside the NCP gateway process / execution environment. This should be the case for national infrastructure security also, meaning that no unencrypted patient data SHOULD be disclosed in the NCP ZONE outside the NCP gateway (impact on gateway application design), see figure below.</p> <p>NCP contains PDP, PEP &amp; STS.</p> <p>NCP zone should be on the inside of public DMZ zone in MS setup</p>	<p>Simple packet filtering for incoming requests.</p>
Firewall towards internet	<p>Firewall that provide protection for the NCP and indirectly the national infrastructure. It should be a hardened platform.</p> <p>It can be implemented as more than one system.</p>	<p>Hardened platform</p> <p>Address, Port, Packet filtering</p> <p>Stateful Web Service proxy</p> <p>Active security mechanisms &amp; intrusion detection</p>
Firewall towards nat. inf.	<p>Firewall that provide protection for the national infrastructure and as a filter protection for the epSOS network</p>	<p>Hardened platform</p> <p>Address, Port, Packet filtering</p>
Firewall (centr.serv.)	<p>Firewall that provide protection for the epSOS central services, which should provide the same security level as the "Firewall towards Internet"</p> <p>The firewall is redundant if the central services are virtual, i.e. follow the p2p pattern, and the central services are placed in the NCP-zone or better.</p>	<p>Same as "Firewall towards Internet"</p>

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010


#### 4.4.2 NCP Gateway Application

The NCP MUST terminate the layer 4+ (SSL/TLS) on the NCP gateway platform inside the NCP gateway process / execution environment. This should be the case for national infrastructure security also, meaning that no unencrypted patient data SHOULD be disclosed in the NCP ZONE outside the NCP gateway (impact on gateway application design), see figure below.



**Figur 1 NCP Application Security**

The figure show the NCP Gateway application process, which needs to include the national & epSOS security termination to secure that no disclosure of data is done out-side the applications security domain (secure memory). It is recommended, that the NCP gateway is started in a secure way, EX: By start with user account, that changes password on start-up.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

## 5 Components Design

This section contains the individual description of the components and a further decomposition of the solution for the NCP.

### 5.1 Inbound Protocol Terminator

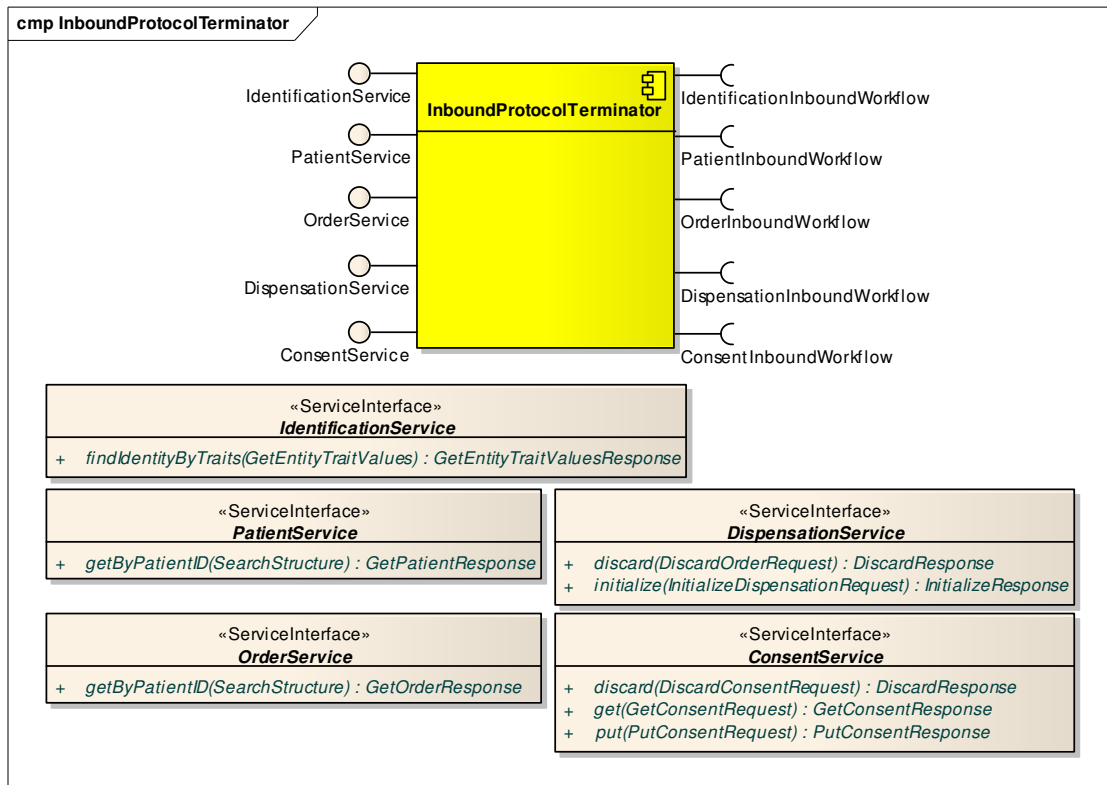



Figure 28 InboundProtocolTerminator component

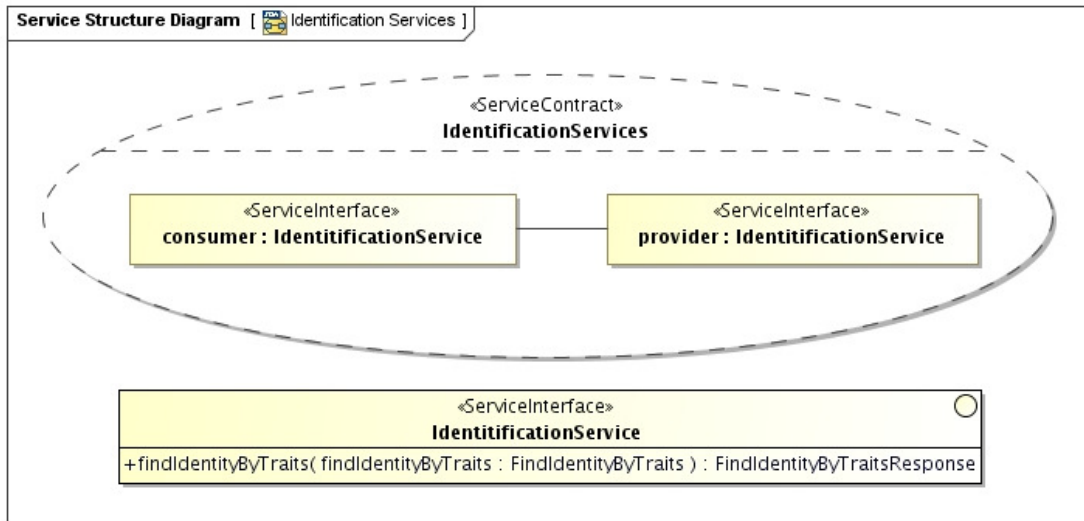
The *InboundProtocolTerminator* component is responsible for providing SOAP web services. It performs verification of WS-Security SAML tokens and deserialization of SOAP message into Java objects. The resulting objects are passed to the *WorkflowManager* who passes them further to the corresponding components. When the *WorkflowManager* returns the resulting object, the *InboundProtocolTerminator* serializes the object in to a SOAP message and passes it as a SOAP response to the corresponding NCP.

#### 5.1.1 epsOS Patient Identification Service

In order to discover a patient's data the patient must be identified and a unique patient identifier must be shared between the communicating gateways. This shared identifier enables the medical data consuming services to properly reference that patients data which is provided by the medical data providing services at the patient's country of affiliation.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010


The epSOS Patient Identification Service defines means for the agreement on this shared identifier and for increasing the degree of accuracy of the patient identification means that are used within the country of care. This shared identifier MUST be used as a patient identifier as required by the epSOS medical data exchange services (e. g. patient service and order service). Figure 29 shows the interface of the epSOS Patient Identification Service as defined in [epSOS D3.3.2].



**Figure 29 epSOS Patient Identification Service Interface**

<b>Operation</b>	<code>findIdentityByTraits()</code>
<b>Description</b>	Obtain a shared patient identifier
<b>Requestor</b>	Consuming Gateway at NCP-B (service consumer at the country of care)
<b>Input Message</b>	FindIdentityByTraitsRequest
Body	(1) List of patient identity traits as provided by the patient to the HCP. (2) optional: minimum confidence level that has to be met by the entities that match the provided traits.
Security Token <sup>3</sup>	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion
<b>Output Message in successful Case</b>	FindIdentityByTraitsResponse
Body	(1) Unique identifier of the patient that has to be used for all subsequent calls for this patient's medical data. (2) optional: further patient identity traits that allow the HCP to verify the result of this operation.  If no unique match is found, the service provider MAY respond with a list of candidates. For each candidate body elements (1) and (2) MUST be provided.
Security Token	[PT] X.509 NCP-A service certificate

<sup>3</sup> PT = Protection Token, ST = Supporting Token

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

**Precondition of success scenario**

1. The service consumer is able to locate the service provider
2. A secure channel is established between service consumer and service provider nodes
3. The service provider is able to verify the authenticity of the service consumer
4. An HCP identity assertion has been issued for the requesting HCP
5. The service provider is able to verify the validity of the HCP identity assertion
6. the service consumer is able to verify the authenticity of the service provider
7. The patient has given a consent that authorises NCP-A to disclose his identity

**Main success scenario**


- Actions of the *epSOS Identification Service* provider:
1. validate the authenticity of the service consumer
  2. verify HCP identity assertion
  3. verify that the requesting HCP is authorised to query for patient IDs
  4. extract the patient identity traits from the message body
  5. search for patients that match the provided ID attributes
  6. discard all patients from the candidates list who have not given consent to epSOS
  7. if no patient matches: throw respective fault
  8. if multiple patients match: request for more identity traits or provide a list of candidates
  9. if single patient matches: select ID to be used for subsequent requests
  10. apply epSOS protection means to the response message and send it to the requestor

**Fault Conditions**

- Preconditions for a success scenario are not given
- 
- Requesting HCP has insufficient rights to query for a patient's identity
- 
- No matching patient is discovered that gave consent to epSOS
- 
- ID traits are insufficient to find a unique match
- 
- The confidence level of the matches is too low with respect to the level required by the requestor
- 
- Patient identification is only performed in conjunction with patient authentication (e.g. by providing a secret or a reference to a valid STORK authentication)
- 
- Confirming the query would lead to a privacy violation acc. to country A legislation.

### 5.1.2 epSOS Patient Service

The epSOS patient service provides operation for retrieving an identified patient's patient summary. Figure 30 shows the interface of the epSOS patient service as defined in [epSOS D3.3.2].

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

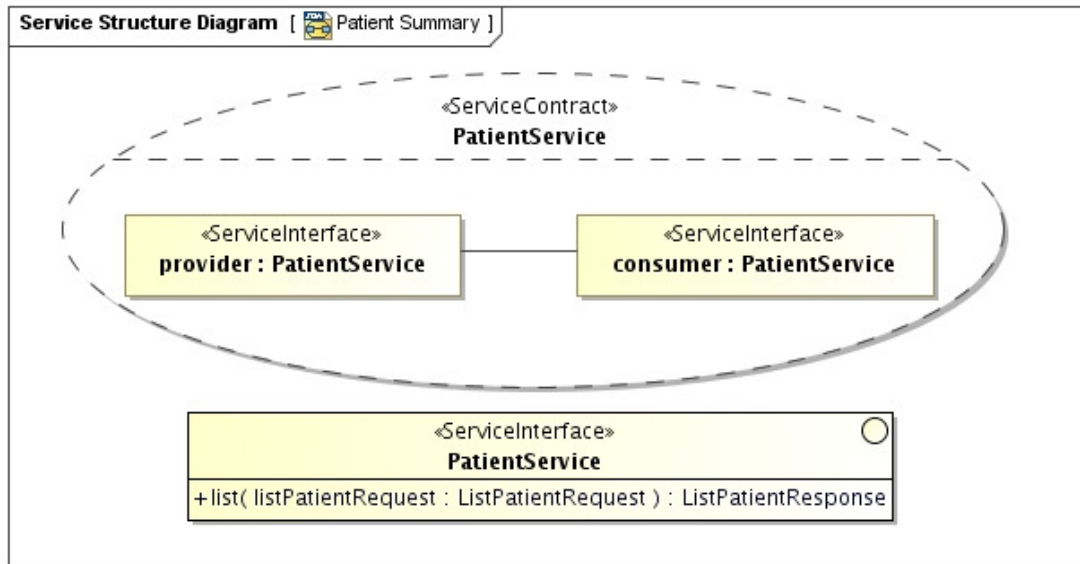



Figure 30 epSOS Patient Service Interface


<b>Operation</b>	list()
<b>Description</b>	Obtain the patient summary of the identified patient
<b>Requestor</b>	Consuming Gateway at NCP-B (service consumer at the country of care)
<b>Input Message</b>	ListPatientRequest
Body	(1) Identifier of the patient whose patient summary is requested (2) Optional: epSOS CDA template qualifier (pivot and/or source coded document). If no template qualifier is given it is up to the service provider to decide if all available encodings or only the epSOS pivot encoding is provided.
Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion
<b>Output Message in successful Case</b>	ListPatientResponse
Body	(1) epSOS-encoded patient summary (CDA) or/and (2) source coded patient summary of the identified patient
Security Token	[PT] X.509 NCP-A service certificate
<b>Precondition of success scenario</b>	<ol style="list-style-type: none"> <li>1. The service consumer is able to locate the service provider</li> <li>2. A secure channel is established between service consumer and service provider nodes</li> <li>3. The service provider is able to verify the authenticity of the service consumer</li> <li>4. service consumer and service provider share a common identifier for the patient</li> <li>5. The patient has given consent to the use of epSOS</li> <li>6. A valid patient summary for the identified patient is accessible for NCP-A</li> <li>7. The requesting HCP has been authenticated in the country of care and the service provider is able to verify the attesting HCP identity assertion</li> <li>8. A treatment relationship exists between the patient and the requesting HCP and the attesting assertion can be verified by the service provider</li> <li>9. the HCP is authorised to access the requested data</li> <li>10. the service consumer is able to verify the authenticity of the service provider</li> </ol>

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name:	NCP - HLDD
		Version:	1.0
	JWG 3.8/3.9: Joint Working Group	Date:	14/05/2010

<b>Main success scenario</b>	Actions of the epSOS Patient Service provider: <ol style="list-style-type: none"> <li>1. validate the authenticity of the service consumer</li> <li>2. verify HCP identity assertion and TRC assertion</li> <li>3. verify that the patient has given valid consent to epSOS and that the consent applies to the recent usage scenario</li> <li>4. retrieve patient's patient summary source document</li> <li>5. enforce national security policy and (if available) patient privacy policy</li> <li>6. verify authenticity and integrity of the patient summary</li> <li>7. transform patient summary into epSOS pivot format (if requested and needed)</li> <li>8. render PDF from source document (if requested and needed)</li> <li>9. apply epSOS protection means to the response message and send it to the requestor</li> </ol>
<b>Fault Conditions</b>	Preconditions for a success scenario are not given Requestor has insufficient rights to access the patient's medical summary No patient summary is available for the identified patient No consent for patient summary sharing is registered for the identified patient The patient summary cannot be provided in the requested encoding Temporary failure (e. g. verification of preconditions cannot be performed due to a system failure)
<b>Warning Conditions</b>	Country A allows for data hiding; a respective disclaimer SHOULD be shown to the HCP The HCP MUST additionally consider the source coded document because this MAY contain additional information The computation of the epSOS encoded patient summary was not approved by an HCP; a respective disclaimer MUST be shown to the requesting HCP The original data (provided as source coded document) was totally or in parts assembled automatically and has not been approved by a HCP; a respective disclaimer MUST be shown to the requesting HCP

### 5.1.3 epSOS Order Service

The epSOS order service provides operation for retrieving an identified patient's available ePrescriptions. Figure 31 shows the interface of the epSOS order service as defined in [epSOS D3.3.2].

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

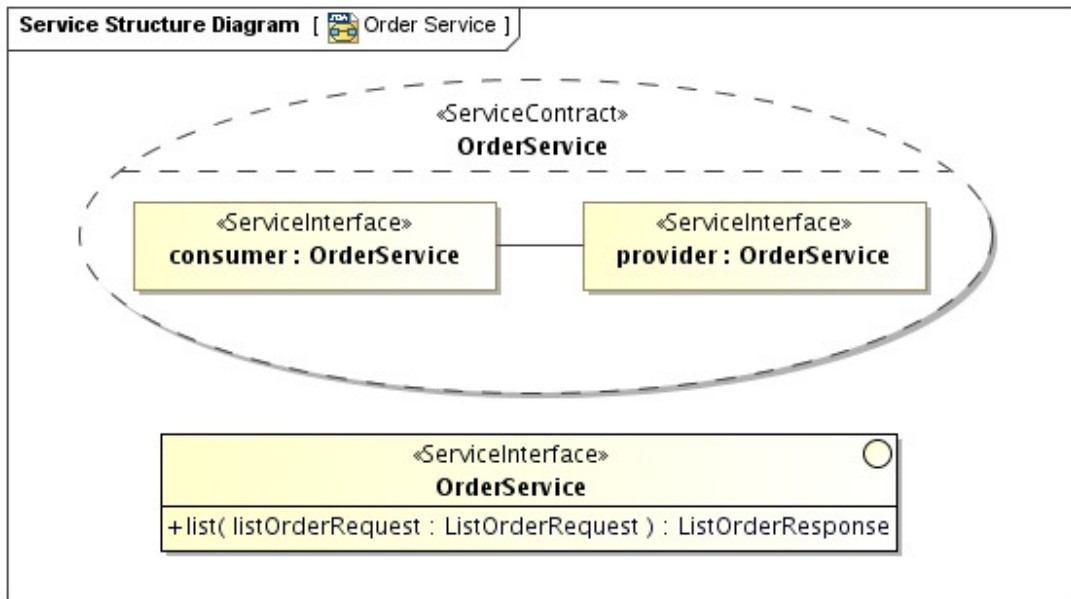



Figure 31 epSOS Order Service Interface

<b>Operation</b>	list()	
<b>Description</b>	Obtain the epSOS-encoded, available ePrescriptions of the identified patient	
<b>Requestor</b>	Consuming Gateway at NCP-B (service consumer at the country of care)	
<b>Input Message</b>	ListOrderRequest	
	Body	(1) Identifier of the patient whose available ePrescriptions are requested (2) Optional: epSOS CDA template qualifier (pivot and/or source coded documents). If no template qualifier is given the service provider MUST respond with all available encodings of the requested documents.
	Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion
<b>Output Message in successful Case</b>	ListOrderResponse	
	Body	(1) List of (1a) epSOS-encoded ePrescriptions and/or (1b) source coded ePrescriptions (acc. to requested format) Of the identified patient
	Security Token	[PT] X.509 NCP-A service certificate
<b>Precondition of success scenario</b>	<ol style="list-style-type: none"> <li>1. The service consumer is able to locate the service provider</li> <li>2. A secure channel is established between service consumer and service provider nodes</li> <li>3. The service provider is able to verify the authenticity of the service consumer</li> <li>4. service consumer and service provider share a common identifier for the patient</li> <li>5. The patient has given consent to the use of epSOS</li> <li>6. All available ePrescriptions for the identified patient are accessible for NCP-A</li> <li>7. The requesting HCP has been authenticated in the country of care and the service provider is able to verify the attesting HCP identity assertion</li> <li>8. A treatment relationship exists between the patient and the requesting HCP and the attesting assertion can be verified by the service provider</li> <li>9. the HCP is authorised to access the requested data</li> <li>10. the service consumer is able to verify the authenticity of the service provider</li> </ol>	




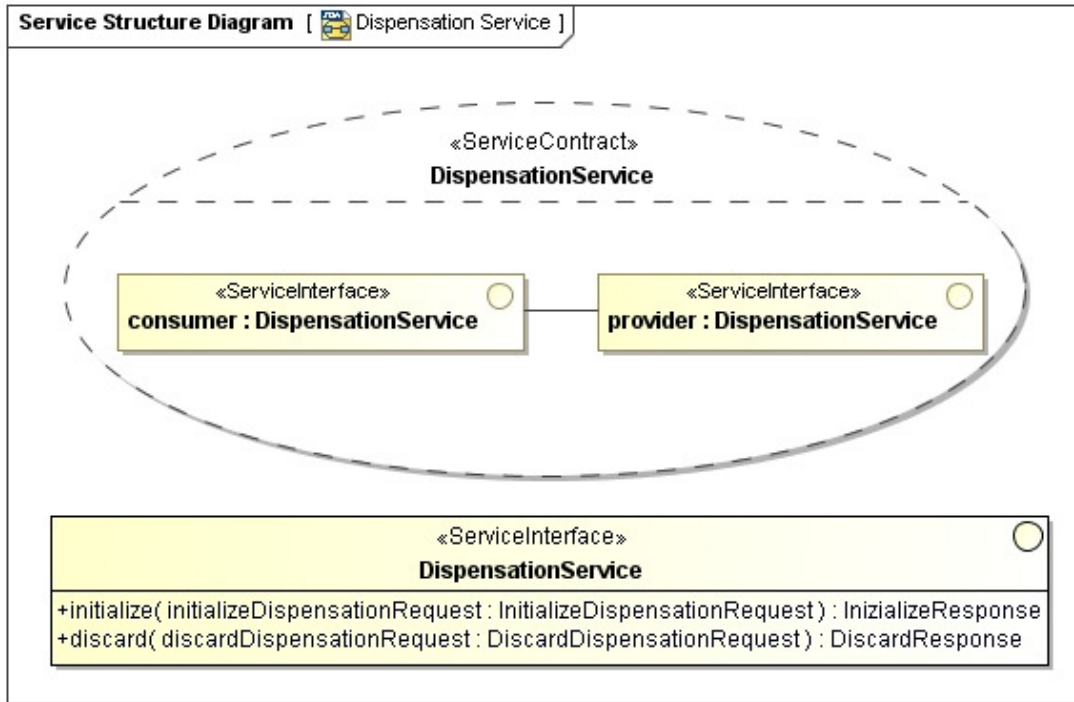
	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>Main success scenario</b>	Actions of the epSOS Order Service provider: <ol style="list-style-type: none"> <li>1. validate the authenticity of the service consumer</li> <li>2. verify HCP identity assertion and TRC assertion</li> <li>3. verify that the patient has given valid consent to epSOS and that the consent applies to the recent usage scenario</li> <li>4. retrieve patient's available prescriptions source documents</li> <li>5. enforce national security policy and (if available) patient privacy policy</li> <li>6. verify authenticity and integrity of the patient summary</li> <li>7. transform ePrescriptions into epSOS pivot format (if requested and needed)</li> <li>8. render PDF from source document (if requested and needed)</li> <li>9. apply epSOS protection means to the response message and send it to the requestor</li> </ol>
<b>Fault Conditions</b>	Preconditions for a success scenario are not given Requestor has insufficient rights to access the patient's ePrescriptions No dispensable ePrescriptions are available for the identified patient No consent for ePrescription sharing is registered for the identified patient A (referenced) ePrescription cannot be provided in the requested encoding Temporary failure (e. g. authenticity verification cannot be performed due to a PKI failure)
<b>Warning Conditions</b>	Country A allows for data hiding; a respective disclaimer SHOULD be shown to the HCP Country A legislation assigns the task of checking for contraindications and drug interaction to the dispenser. A warning MUST be shown to the HCP in country B that the checks for contraindication and drug interaction MAY not have been performed on the prescribed medication in country A. Mandatory fields have been nullified for some of the provided ePrescriptions (minimum dataset is not fully provided); the HCP MUST additionally consider the source coded document More ePrescriptions MAY be available but are not accessible The computation of the CDA encoded ePrescription documents was not approved by an HCP; a respective disclaimer MUST be shown to the HCP A (referenced) ePrescription is time valid for dispensation but not for reimbursement. A message SHOULD be shown to the HCP that he SHOULD inform the patient that his health insurance will not reimburse the dispensed medicine.

### 5.1.4 epSOS Dispensation Service


The epSOS dispensation service provides operations for notifying the patient's country of affiliation on the dispensation of an ePrescription. Figure 32 shows the interface of the epSOS dispensation service as defined in [epSOS D3.3.2].

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010



**Figure 32 epSOS Dispensation Service Interface**

<b>Operation</b>	initialize()						
<b>Description</b>	Notify the patient's country of affiliation on a successful dispensation of an ePrescription						
<b>Requestor</b>	Consuming Gateway at NCP-B (service consumer at the country of care)						
<b>Input Message</b>	initializeDispensationRequest						
	<table border="1"> <tr> <td>Body</td> <td>(1) epSOS coded eDispensation documents as defined by [epSOS D3.5.2]. (2) source coded dispensation data</td> </tr> <tr> <td></td> <td>The body MUST contain at least one epSOS pivot coded dispensation document (1). It MUST contain at least one source coded document (2). There MUST be a 1:1 association among provided source coded documents and epSOS coded eDispensation documents.</td> </tr> <tr> <td>Security Token</td> <td>[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion</td> </tr> </table>	Body	(1) epSOS coded eDispensation documents as defined by [epSOS D3.5.2]. (2) source coded dispensation data		The body MUST contain at least one epSOS pivot coded dispensation document (1). It MUST contain at least one source coded document (2). There MUST be a 1:1 association among provided source coded documents and epSOS coded eDispensation documents.	Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion
Body	(1) epSOS coded eDispensation documents as defined by [epSOS D3.5.2]. (2) source coded dispensation data						
	The body MUST contain at least one epSOS pivot coded dispensation document (1). It MUST contain at least one source coded document (2). There MUST be a 1:1 association among provided source coded documents and epSOS coded eDispensation documents.						
Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion						
<b>Output Message in successful Case</b>	initializeDispensationResponse						
	<table border="1"> <tr> <td>Body</td> <td>(1) Success indicator</td> </tr> <tr> <td>Security Token</td> <td>[PT] X.509 NCP-A service certificate</td> </tr> </table>	Body	(1) Success indicator	Security Token	[PT] X.509 NCP-A service certificate		
Body	(1) Success indicator						
Security Token	[PT] X.509 NCP-A service certificate						

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>Precondition of success scenario</b>	<ol style="list-style-type: none"> <li>1. The service consumer is able to locate the service provider</li> <li>2. A secure channel is established between service consumer and provider nodes</li> <li>3. The service consumer is able to verify the authenticity of the service provider</li> <li>4. Service consumer and service provider share a common identifier for the patient</li> <li>5. The patient has given consent to the use of epSOS</li> <li>6. The service consumer has previously retrieved the list of the patient's available ePrescriptions</li> <li>7. All available ePrescriptions for the identified patient are accessible for NCP-A and the provided eDispensation data relates to these ePrescriptions</li> <li>8. The requesting HCP has been authenticated in the country of care and the service provider is able to verify the attesting HCP identity assertion</li> <li>9. A treatment relationship exists between the patient and the requesting HCP and the attesting assertion can be verified by the service provider</li> <li>10. The HCP is authorised to dispense medication for the patient</li> </ol>
---	--

<b>Main success scenario</b>	Actions of the epSOS Dispensation Service provider: <ol style="list-style-type: none"> <li>1. Validate the authenticity of the service consumer</li> <li>2. Verify HCP identity assertion and TRC assertion</li> <li>3. Verify that the patient has given consent to epSOS and that the consent is valid</li> <li>4. Enforce national security policy and (if available) patient privacy policy</li> <li>5. Verify that all dispensation information is provided and that dispensation data is properly coded</li> <li>6. Retrieve patient's available prescriptions and verify that each dispensation item matches with a prescribed item</li> <li>7. Process the dispensation information (optional)</li> <li>8. Apply epSOS security measures to the success indicator and send it to the requestor</li> </ol>
------------------------------	---

<b>Fault Conditions</b>	Preconditions for a success scenario are not given <hr/> The requesting HCP has insufficient rights to dispense the identified patient's ePrescriptions <hr/> One or more of the provided dispensation items do not relate to available ePrescriptions of the identified patient <hr/> No consent for ePrescription sharing and dispensing is registered for the identified patient <hr/> The eDispensation data is not provided in all mandatory encodings <hr/> Temporary failure (e.g. verification of a signature cannot be performed due to a PKI failure)
-------------------------	--

<b>Warning Conditions</b>	eDispensation data is not processed by the patient's country of affiliation
---------------------------	---


<b>Operation</b>	Discard()
------------------	-----------

<b>Description</b>	Notify the patient's country of affiliation on an erroneous eDispensation notification, in order to allow it to rewind any changes made on its internal data that were triggered by the erroneous notification
--------------------	--

<b>Requestor</b>	Consuming Gateway at NCP-B (service consumer at the country of care)
------------------	--

<b>Input Message</b>	discardDispensationRequest
Body	(1) Identifier of the eDispensation document that is to be discarded
Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion

<b>Output Message in successful Case</b>	discardDispensationResponse
Body	Success indicator
Security Token	[PT] X.509 NCP-A service certificate

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

**Precondition of success scenario**

1. The service consumer is able to locate the service provider
2. A secure channel is established between service consumer and provider nodes
3. The service consumer is able to verify the authenticity of the service provider
4. Service consumer and service provider share a common identifier for the patient
5. The patient has given consent to the use of epSOS
6. The service consumer has previously retrieved the list of the patient's available ePrescriptions and dispensed the identified medicine
7. The requesting HCP has been authenticated in the country of care and the service provider is able to verify the attesting HCP identity assertion

**Main success scenario**

- Actions of the epSOS Dispensation Service provider:
1. Validate the authenticity of the service consumer
  2. Verify HCP identity assertion
  3. Extract the dispensed item id from the message body and ensure that this item was previously dispensed by the identified HCP
  4. Enforce national security policy and (if available) patient privacy policy
  5. Rewind the dispensation (optional)
  6. Sign the success notification and send it to the requestor

**Fault Conditions**


- Preconditions for a success scenario are not given
- 
- The HCP has insufficient rights to process the patient's ePrescription data
- 
- The HCP was not the original dispenser of the identified medication item
- 
- The identified item had not been dispensed previously
- 
- Temporary failure (e.g. service provider is temporarily unable to access an internal service)

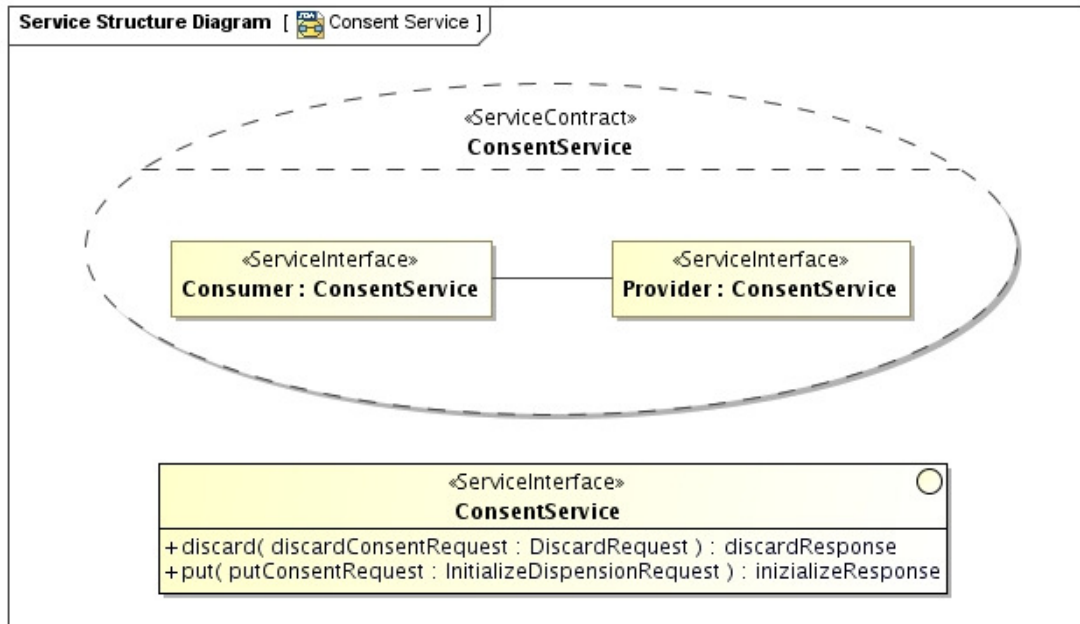
**Warning Conditions**

- eDispensation data is not processed by the country of affiliation
- 
- eDispensations are not rolled back automatically by the country of affiliation

### 5.1.5 Consent Service


The epSOS consent service provides operations for the remote management of consents (e. g. giving and revoking consent from abroad). Figure 33 shows the interface of the epSOS patient service as defined in [epSOS D3.3.2].

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010




**Figure 33 epSOS Consent Service Interface**

<b>Operation</b>	put ( )
<b>Description</b>	Notify the patient's country of affiliation on a consent newly given or revoked in the country of care. The consent status modification only applies to the country of care.
<b>Requestor</b>	Consuming Gateway at NCP-B (service consumer at the country of care)
<b>Input Message</b>	putConsentRequest
Body	(1) Information on the newly given or revoked consent (2) Optional: signed (scanned) consent document
Security Token	[PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion [ST] epSOS Treatment Relationship Confirmation Assertion
<b>Output Message in successful Case</b>	putConsentResponse
Body	Status of the consent (given/revoked)
Security Token	[PT] X.509 NCP-A service certificate
<b>Precondition of success scenario</b>	<ol style="list-style-type: none"> <li>1. The service consumer is able to locate the service provider</li> <li>2. A secure channel is established between service consumer and provider nodes</li> <li>3. The service consumer is able to verify the authenticity of the service provider</li> <li>4. The service provider is able to verify the authenticity of the service consumer</li> <li>5. Service consumer and service provider share a common identifier for the patient</li> <li>6. The requesting HCP has been authenticated in the country of care and the service provider is able to verify the attesting HCP identity assertion</li> <li>7. The patient has confirmed in the consent status change</li> </ol>
<b>Main success scenario</b>	Actions of the epSOS Consent Service provider: <ol style="list-style-type: none"> <li>1. Validate the authenticity of the service consumer</li> <li>2. Verify HCP identity assertion</li> <li>3. Verify that the requested status change is allowed by country-A security policies</li> <li>4. verify that the patient has given a general consent to epSOS (implied or explicit)</li> <li>5. Apply the consent status change for the country of care</li> <li>6. Sign the success indicator and send it to the requestor</li> </ol>

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>Fault Conditions</b>	Preconditions for a success scenario are not given
	Security policy violation (e.g. the HCP's role is not permitted to mediate consent changes)
	A patient authentication is required (e.g. by signing the consent document)
	Country-A legislation requires that a scanned consent document is provided with the request
	Temporary failure (e.g. service provider is temporarily unable to access an internal service)
<b>Warning Conditions</b>	Consent status change requests are not processed by the country of affiliation
	Consent status changes are not applied automatically by the country of affiliation. Therefore the consent status change will not be immediately operative.
<b>Operation</b>	Discard()
<b>Description</b>	Notify the patient's country of affiliation on an erroneous consent status change notification, in order to allow it to rewind any changes made on its internal data that were triggered by the erroneous notification
<b>Requestor</b>	Consuming Gateway at NCP-B (service consumer at the country of care)
<b>Input Message</b>	discardConsentRequest
	Body (1) Identifier of the consent status document that is to be discarded
	Security Token [PT] X.509 NCP-B service certificate [ST] epSOS HCP Identity Assertion
<b>Output Message in successful Case</b>	discardConsentResponse
	Body Status of the consent (given/revoked)
	Security Token [PT] X.509 NCP-A service certificate
<b>Precondition of success scenario</b>	<ol style="list-style-type: none"> <li>1. The service consumer is able to locate the service provider</li> <li>2. A secure channel is established between service consumer and provider nodes</li> <li>3. The service consumer is able to verify the authenticity of the service provider</li> <li>4. The service consumer has previously triggered a consent change and is responsible for the consent document that is to be discarded</li> <li>5. The requesting HCP has been authenticated in the country of care and the service provider is able to verify the attesting HCP identity assertion</li> </ol>
<b>Main success scenario</b>	Actions of the epSOS Consent Service provider: <ol style="list-style-type: none"> <li>1. Validate the authenticity of the service consumer</li> <li>2. Verify HCP identity assertion</li> <li>3. Extract the consent document id from the message body and ensure that this consent status change was previously triggered by the identified HCP</li> <li>4. Enforce national security policy and (if available) patient privacy policy</li> <li>5. Rewind the consent giving/revocation (optional)</li> <li>6. Sign the success notification and send it to the requestor</li> </ol>
<b>Fault Conditions</b>	Preconditions for a success scenario are not given
	Country-A legislation does not allow for discarding a consent; a new consent is required
	The HCP was not the original mediator of the identified consent document
	The identified document is not known
	Temporary failure (e.g. service provider is temporarily unable to access an internal service)
<b>Warning Conditions</b>	Consent status change requests are not processed by the country of affiliation
	Consent status changes are not rolled back automatically by the country of affiliation

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

## 5.2 Outbound Protocol Terminator

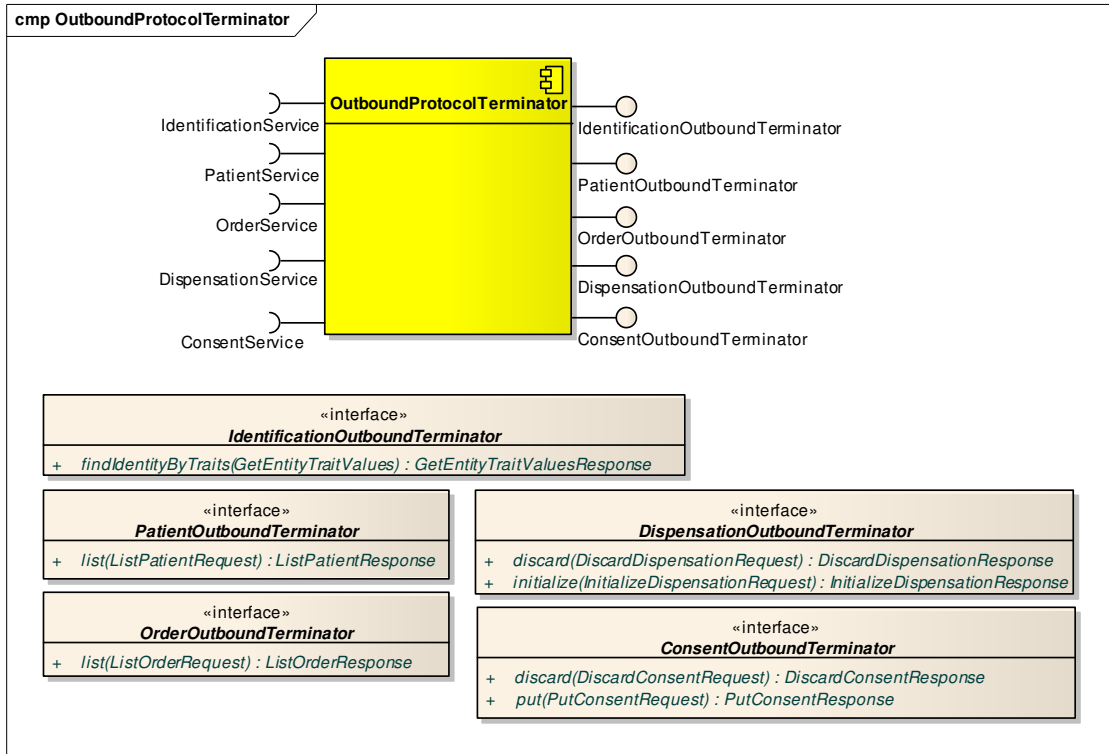



Figure 34 OutboundProtocolTerminator component

The *OutboundProtocolTerminator* plays the 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 in a Java message object and transfers the object to the *WorkflowManager*.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

### 5.3 Workflow Manager

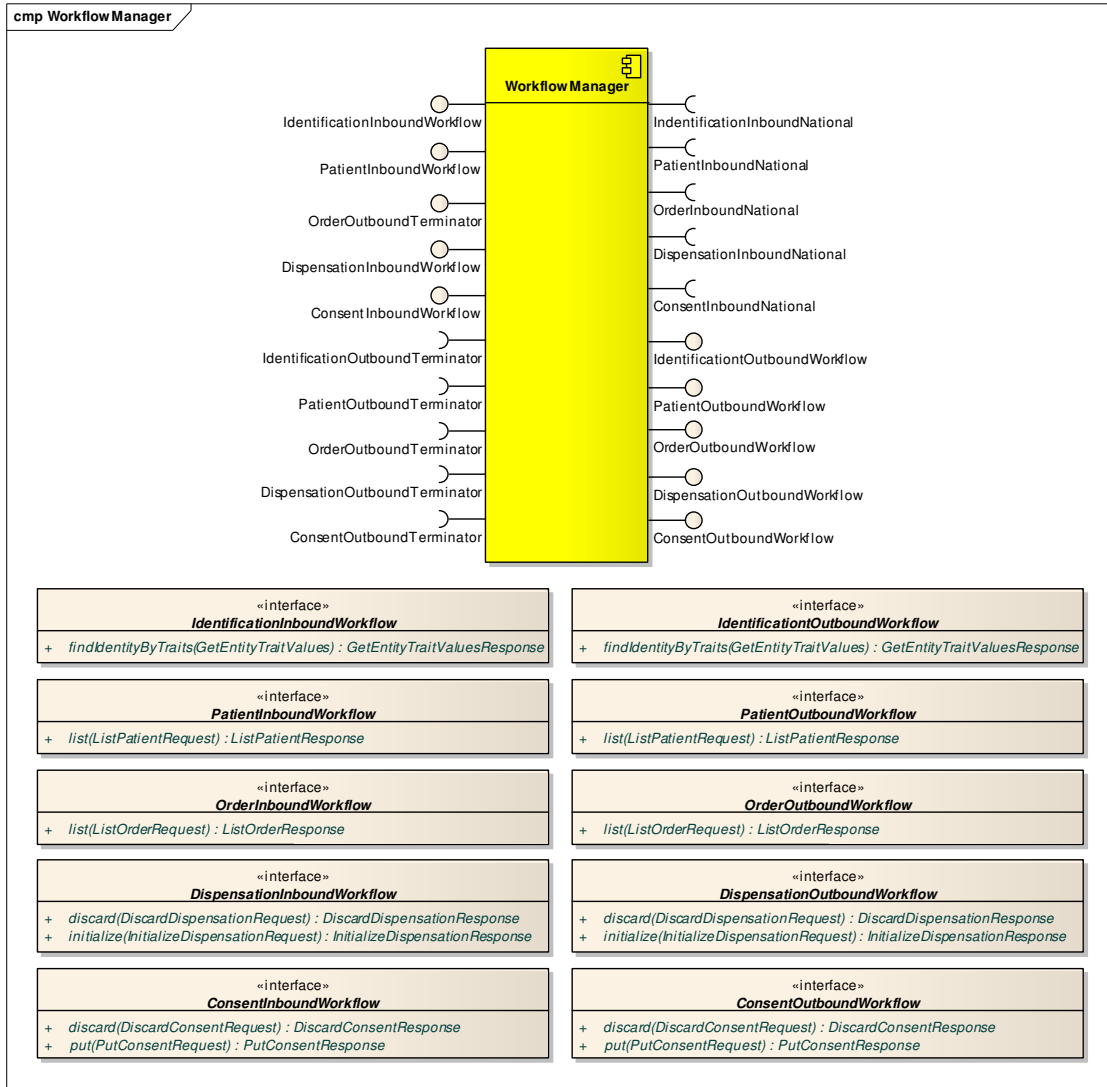



Figure 35 WorkflowManager component

Conducts the invocation of components to process a request. The *WorkflowManager* has 2 possible modes:

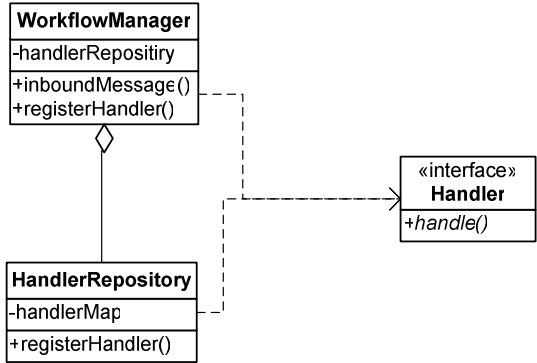
- a) Dispatch to configured functions. This option sees a sequencer controlled by a configuration table, which will call standards functions, passing the message object to business functions with generic interfaces.
- b) Dispatch to registered functions. This approach allows components to register as handlers for specific message types, that itself will call business functions with specialized interfaces.

For the time being, approach b) was chosen. The approach is briefly presented in the next section.



	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

### 5.3.1 Handler Interface



The handlers encapsulate business transactions and implement a *Handler* interface. This interface decouples the *WorkflowManager* from the actual handlers.

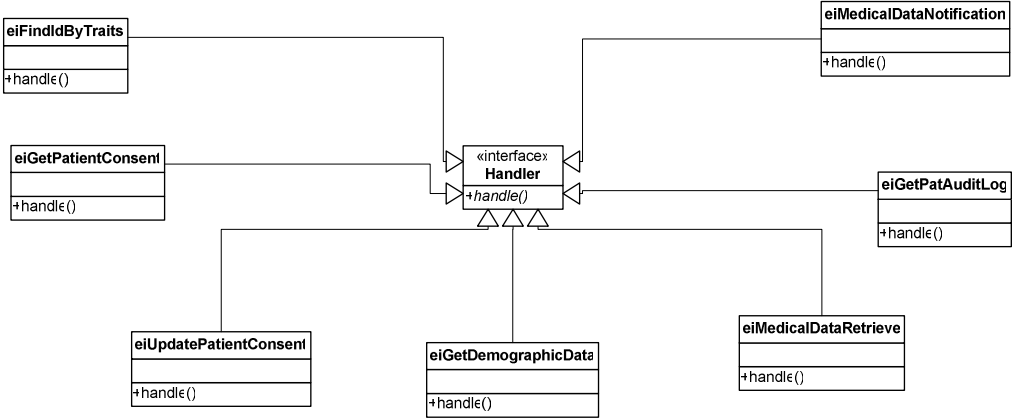



Figure 36 Handler interface and example of implementations

### 5.4 Audit Trail Writer

This *AuditTrailWriter* component is responsible for formatting an *EventLog* message in an Audit Trail and Node Authentication (ATNA) -compatible way, and pass it securely to the audit repository.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

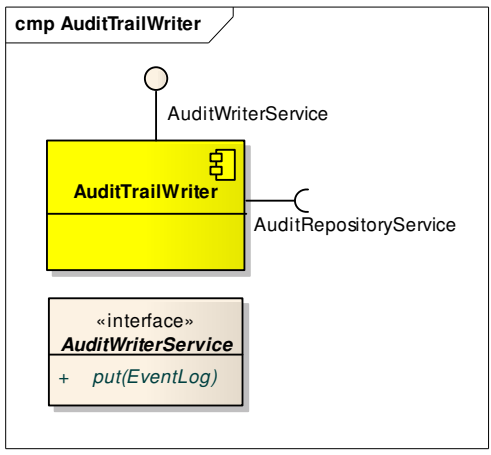


Figure 37 AuditTrailWriter component

**put (EventLog)**

<b>Textual description of operation</b>	
This operation stores an audit event in the audit trail.	
<b>Input parameters</b>	<b>EventLog</b> Audit entry to record in a format which is yet to define
<b>Output parameters</b>	-
<b>Notes</b>	No identifiable medical information should be contained in EventLog

**5.5 Audit Repository**

The *AuditRepository* component is responsible for storing audit trail entries in an ATNA-compatible way. The content of the audit repository will be analyzed in the national infrastructure. Therefore, presented here the *AuditService* interface has a very general structure that can be further adjusted by member states according to their specific needs.

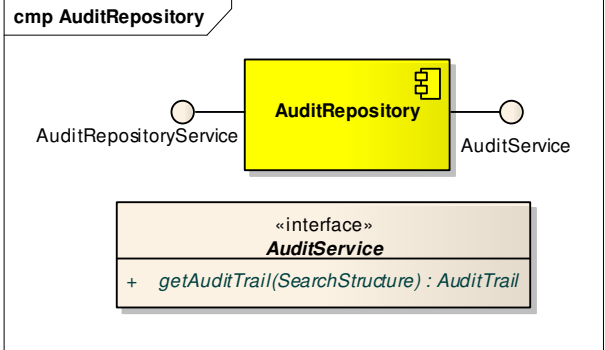



Figure 38 AuditRepository component

**getAuditTrail (SearchStructure) : AuditTrail**

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010

<b>Textual description of operation</b>	
The operation allows to selectively extract records from the audit trail	
<b>Input parameters</b>	<b>SearchStructure</b> The structure contains search parameters that define which records of the audit trail should be extracted
<b>Output parameters</b>	<b>AuditTrail</b> Records of the audit trail that correspond to the parameters defined in SearchStructure
<b>Notes</b>	No identifiable medical information should be contained in the audit repository

## 5.6 Security Manager

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

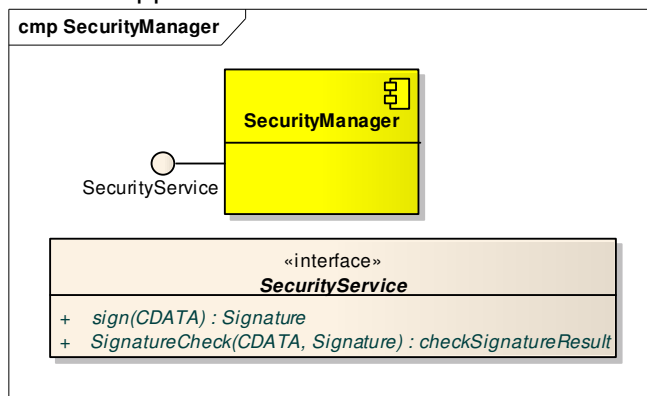



Figure 39 SecurityManager component

**sign(CDATA) : Signature**

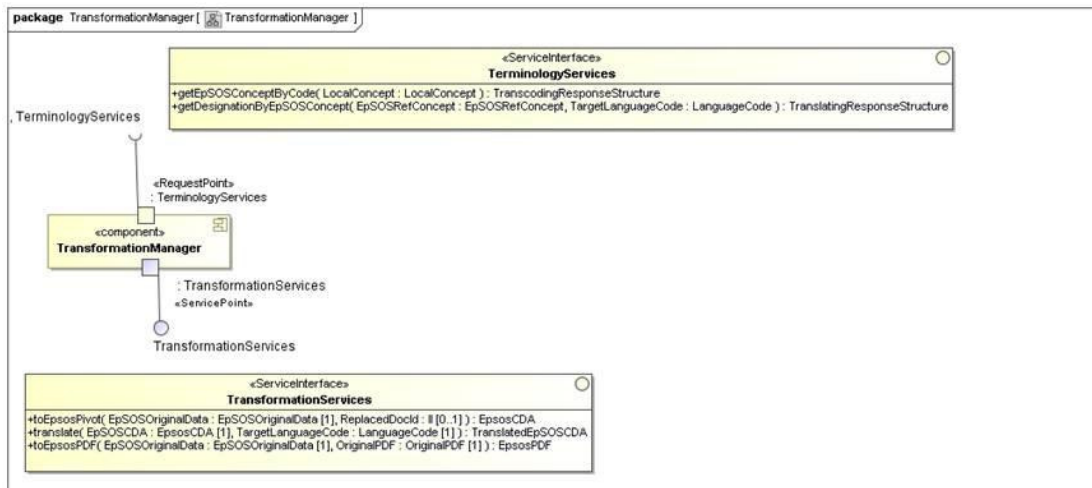
<b>Textual description of operation</b>	
This operation processes a XML DSig signature for a given XML according to the XML DSig standard and the epSOS profilation. Only known documents are signed and before the signature processing a schema validation is done. The documents that are known are configurable.	
<b>Input parameters</b>	<b>CDATA</b> XML Document to sign
<b>Output parameters</b>	<b>Signature</b>
<b>Notes</b>	In case it is decided that it is enough to provide WS-signatures, this functionality can be discarded

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

**CheckSignature (CDATA, Signature) : CheckSignatureResult**

<b>Textual description of operation</b>	
The XML DSign signature of a XML document is validated including the validation of the certificate that confirmed the signature.	
<b>Input parameters</b>	<b>CDATA</b> XML containing <b>Signature</b> Digital signature
<b>Output parameters</b>	<b>CheckSignatureResult</b> Encoded in the status information are <ul style="list-style-type: none"> <li>• Validity of signature</li> <li>• Validity of certificate</li> </ul>
<b>Notes</b>	All the known and trusted certificates have to be registered by configuration beforehand. In case it is decided that it is enough to provide WS-signatures, this functionality can be discarded


## 5.7 Transformation Manager



**Figure 40 – Component : TransformationManager**

### Component responsibilities

- Translating and/or transcoding (if necessary) the original data compliant to epSOS CDA syntax from the national language and possibly from the national code system(s) in the document creator country (in most cases Country A) to the epSOS Reference Terminology. From a functional point of view the translation and transcoding are the same operation for the


	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

Transformation Manager from the point of view of the document creator country (in most cases Country A).

- Creating an epSOS unstructured CDA by embedding the original data from document creator presented in the pdf format. Note: the assumption is made that the original data is already presented in a pdf format. The document creator country may have other formats internally; however this data must be presented in a pdf format so that the document consumer country can read it. If, for whatever reasons, the original data needs to be sent, it can be processed in a similar way. However, for the pilot purposes only the pdf operation is defined.
- Translating the coded data elements from the epSOS Reference Terminology to the national language in document consumer country (in most cases Country B).

**ToEpSOSPivot (EpSOSOriginalData; ReplacedDocId) :EpsosCDA**


<b>Textual description of operation</b>	
Transformation of national data to epSOS pivot format.	
<b>Input parameters</b>	<b>EpSOSOriginalData</b> Medical document in its original data format as provided from the NationalConnector to this component. The provided document is compliant with the epSOS pivot CDA (see D 3.5.2 Appendix C) unless the adoption of the element binding with the epSOS reference Value Sets. [Mandatory]  <b>ReplacedDocId</b> is an instance identifier describing the document to be replaced.
<b>Output parameters</b>	<b>EpSOSCDA</b> structure Response structure including the epSOS pivot CDA and the response status structure. The response status structure provides information about the operation results, including possible errors and warning.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>Component behaviour</b>	<p>After having received a <i>toEpSOSPivot()</i> request, this component takes the <i>EpSOSOriginalData</i> (already compliant to epSOS CDA syntax) and using the TSAM 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 to have a link to the <i>EpSOSOriginalData</i>.</p> <p><i>Exceptions:</i> in case of processing error or warning, the <i>responseStatusStructure</i> will be used to convey this information to the calling component with an appropriated error and warning code. A detailed list of the managed exceptions will be provided in the Detail Design Specification document. Each exception condition occurred will be logged (standard and audit), reporting both the exception code and its English description.</p>
<b>Notes</b>	

**ToEpSOSPDF (EpSOSOriginalData; OriginalPDF ) : EpSOSPDF**


<b>Textual description of operation</b>	
Transformation of national data to epSOS pivot format.	
<b>Input parameters</b>	<p><b>EpSOSOriginalData</b>          Medical document in its original data format as provided from the NationalConnector to this component.          The provided document is compliant with the epSOS pivot CDA (see D 3.5.2 Appendix C) unless the adoption of the element binding with the epSOS reference Value Sets. [Mandatory]</p> <p><b>OriginalPDF</b>          Printable representation (PDF/A) of the original national data as we expect have been seen by the originator HCP [Mandatory].</p>
<b>Output parameters</b>	<p><b>EpSOSPDF</b> structure          response structure including the epSOS unstructured CDA embedding the original pdf and the response status structure.</p> <p>The response status structure provides information about the operation results, including possible errors and warning.</p>

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>Component behaviour</b>	<p>After having received the <i>ToEpSOSPDF()</i> request, this component takes the <i>EpSOSOriginalData</i> and the <i>OriginalPDF</i> and generates an unstructured CDA embedding the PDF using the information already present in the <i>EpSOS</i> 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 <i>EpSOSOriginalData</i>.</p> <p><i>Exceptions:</i> in case of processing error or warning, the <i>responseStatusStructure</i> will be used to convey this information to the calling component with an appropriated error and warning code. A detailed list of the managed exceptions will be provided in the Detail Design Specification document. Each exception condition occurred will be logged (standard and audit), reporting both the exception code and its English description.</p>
<b>Notes</b>	

**Translate (EpsosCDA; TargetLanguageCode) : TranslatedEpSOSCDA**

<b>Textual description of operation</b>	
Translation from epSOS pivot data to consumer country language.	
<b>Input parameters</b>	<p><b>EpSOSosCDA</b> Document in epSOS pivot format (with epSOS codes )</p> <p><b>TargetLanguageCode.</b> Identifier (code) of the target language.</p>
<b>Output parameters</b>	<b>TranslatedEpSOSCDA</b> epSOS pivot CDA with translated epSOS codes into the consumer country language.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>Component behaviour</b>	<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 to obtain the representation of that concept in the target TargetLanguageCode identifier . This information is therefore used by this component to update the displayName 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 responseStatusStructure will be used to convey this information to the calling component with an appropriated error and warning code. A detailed list of the managed exceptions will be provided in the Detail Design Specification document. Each exception condition occurred will be logged (standard and audit), reporting both the exception code and its English description.</p>
<b>Notes</b>	

### Linking documents

The relationship between the epSOS pivot document and the embedded PDF CDA is always inferred via the XFRM relationship with their parent document EpSOSOriginalData. Optionally, a direct relationship between the epSOS pivot document and the embedded PDF CDA could be created on request as RPLC relationship.

### Component behaviour (called operations)


#### **getEpSOSConceptByCode ( )**

This component issues a getEpSOSConceptByCode\_() request in order to know the best matching epSOS Concept, according to the information provided.

*Exceptions:* in case of returned errors this component shall appropriately use NullFlavors for valorising the “main” coded concept; nevertheless the original code shall be provided through the <translation> element.

#### **getDesignationByEpSOSConcept ( )**



	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

This component issues `getDesignationByEpSOSConcept_()` request in order to know the target language epSOS Designation, according to the information provided.

*Exceptions:* in case of returned errors no actions are required for `displayName` translation.

This component provides capabilities for coded concepts translation and transcoding if necessary.

## 5.8 Terminology Services Access Manager

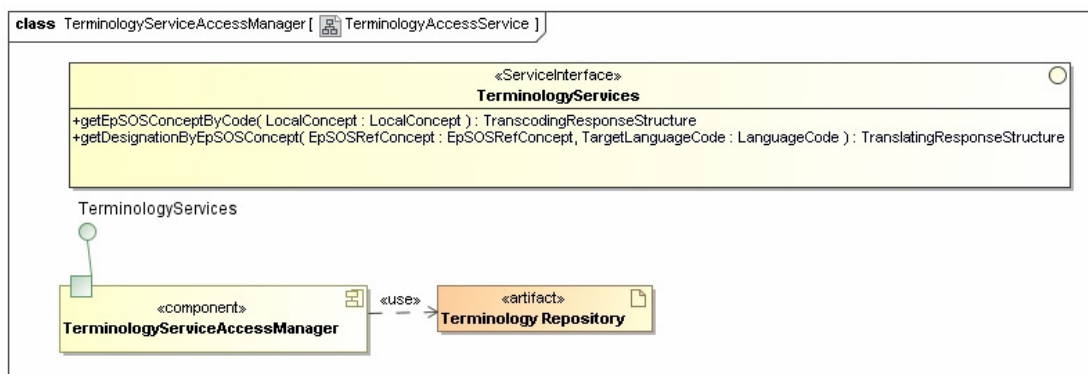
This component provides capabilities for coded concepts translation and transcoding if necessary.

The first term (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.)


With the second term (transcoding) we mean the capability of getting the epSOS quasi-synonymous<sup>4</sup> associated to a “local” coded concept.

In both cases, the content needed by the Terminology Services Access Manager is the Terminology Repository. The Terminology Repository is a database representation of the epSOS Reference Terminology.

It must be noted that the epSOS Reference Terminology has as a starting point the epSOS MVC, which in turn is the basis for the epSOS MTC (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 . This mapping is compiled in the epSOS Master Value Sets Translation/Transcoding Catalogue (epSOS MTC ). The maintenance of the MTC and its relationship with the MVC are out of scope of the common components design.



<sup>4</sup> i.e. a coded concept derived from the appropriate epSOS Value Set semantically equivalent to a given coded concept.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name:	NCP - HLDD
		Version:	1.0
	JWG 3.8/3.9: Joint Working Group	Date:	14/05/2010


**Figure 41 – Component : TerminologyServiceAccessManager**

**Component responsibilities**

1. Translating a given concept designation into the requested target language using the information present in the Terminology Repository.
2. Transcoding a given “local” coded concept into the appropriate epSOS coded concept using the information present in the Terminology Repository.

**getEpSOSConceptByCode (LocalConcept) :**  
**TranscodingResponseStructure**


<b>Textual description of operation</b>	
Transcoding a given “local” coded concept into the appropriate epSOS coded concept using the information present in the Terminology Repository.	
<b>Input parameters</b>	<b>LocalConcept;</b> structure used to convey the concept derived from the epSOS Original Data. It shall include at least the concept code and the concept code system. Code System Version, Country Code and value set OID - if available - should be provided.
<b>Output parameters</b>	<b>TranscodingResponseStructure</b> Response structure including: <ol style="list-style-type: none"> <li>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,</li> <li>2. The responseStatusStructure, providing information about operation result, including possible errors and warning.</li> </ol>

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>Component behaviour</b>	<p>When this component receives a <code>getEpSOSConceptByCode_()</code> request, it uses all the data extracted from the <code>LocalConcept</code> 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). All information retrieved is finally returned to the requesting component.</p> <p><i>Exceptions:</i> if there is no transcoding or a processing error occurs, the <code>ResponseStatusStructure</code> will be used to convey this information to the calling component with an appropriated error and warning code. A detailed list of the managed exceptions will be provided in the Detail Design Specification document. Each exception condition occurred will be logged (standard and audit), reporting both the exception code and its English description.</p>
<b>Notes</b>	Makes use of Terminology Repository

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

<b>Textual description of operation</b>	
Translating a given concept designation into the requested target language using the information present in the Terminology Repository	
<b>input parameters</b>	<p><b>EpSOSRefConcept.</b> Structure used to convey the concept derived from the epSOS pivot CDA. It shall include at least the concept code and the concept code system. Code System Version, Country Code and value set OID - if available - should be provided.</p> <p>TargetLanguageCode identifier (code) of the target language.</p>
<b>Output parameters</b>	<p><b>translatingResponseStructure</b> Response structure including:</p> <ol style="list-style-type: none"> <li>1. the target language concept designation;</li> <li>2. the <code>ResponseStatusStructure</code> providing information about operation result, including possible errors and warning.</li> </ol>


	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

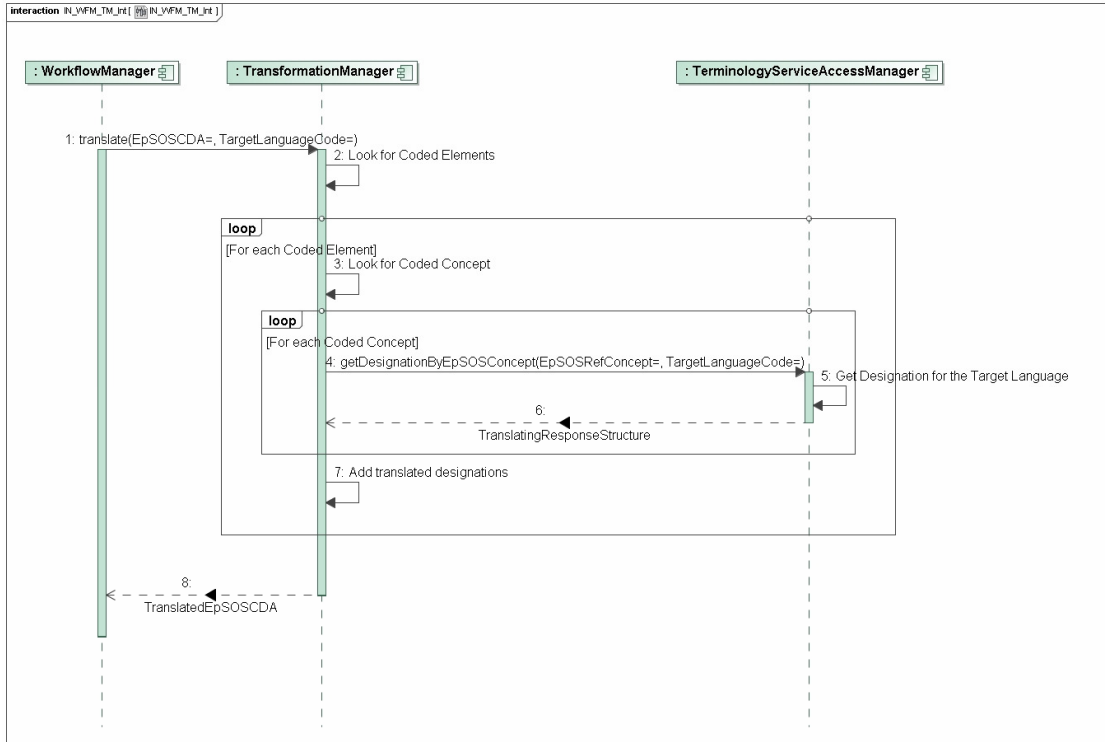
<b>Component behaviour</b>	<p>When this component receives a <code>getDesignationByEpSOSConcept_()</code> request, it uses all the data extracted from the <code>EpSOSRefConcept</code> structure in order to search within the Terminology Repository for the target language <code>epSOS</code> Designation, according to the local information provided (e.g., if no code system version is indicated, the latest version will be provided). All information retrieved are finally returned to the requesting component.</p> <p><i>Exceptions:</i> if there is no translation or a processing error occurs, the <code>responseStatusStructure</code> will be used to convey this information to the calling component with an appropriated error and warning code. A detailed list of the managed exceptions will be provided in the Detail Design Specification document. Each exception condition occurred will be logged (standard and audit), reporting both the exception code and its English description.</p>
<b>Notes</b>	Makes use of Terminology Repository

### 5.8.1 Interaction Uses


This section describes the two NCP “interaction uses” (IU) in which the Semantic Components are involved:

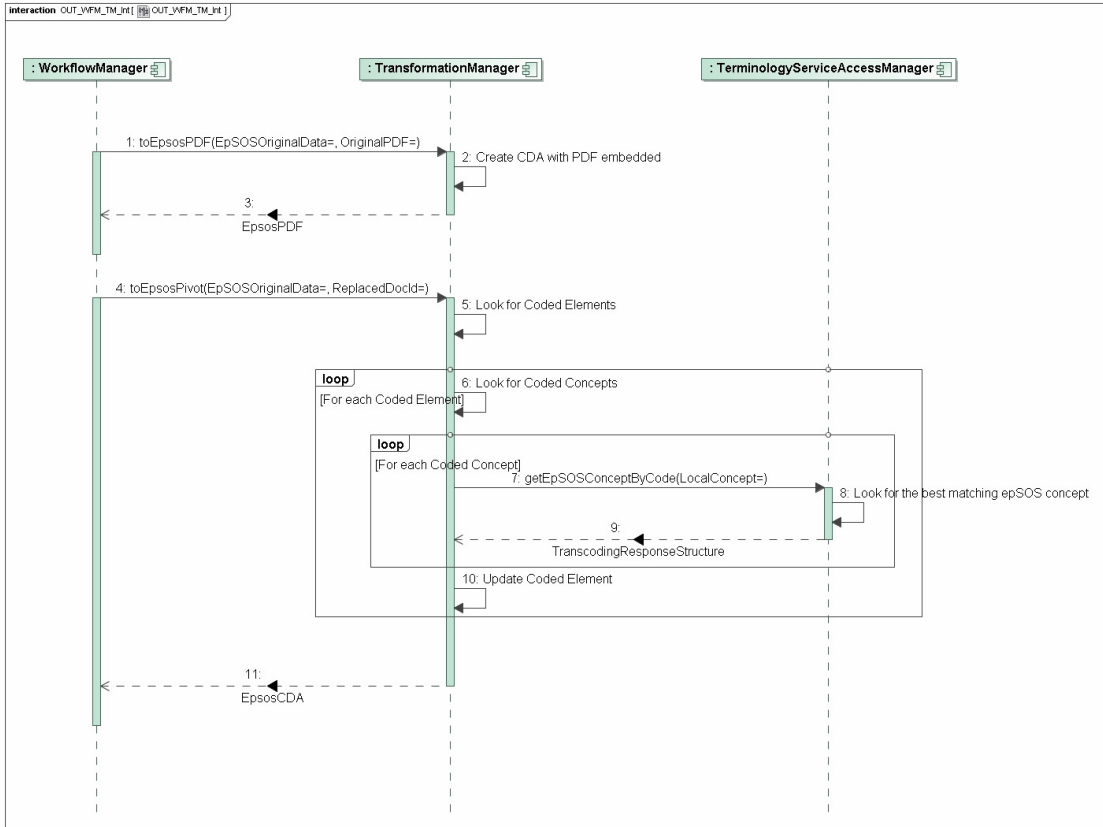
1. The Document Provider Workflow Manager Transformation Manager Interaction Use (`Out_WM_TM_IU`). This IU is performed at a certain time of the workflow by the Document Provider NCP (usually NCP-A) to create the `epSOS` pivot CDA and the CDA with the original PDF embedded.
2. The Document Consumer Workflow Manager Transformation Manager Interaction Use (`In_WM_TM_IU`). This IU is performed at a certain time of the workflow by the Document Consumer NCP (usually NCP-B) to create a translated version of the `epSOS` pivot CDA into the target language.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010



**Figure 42 - Document Consumer WorkflowManager-TransformationManager Interaction Use (IN\_WM\_TM\_IU)**

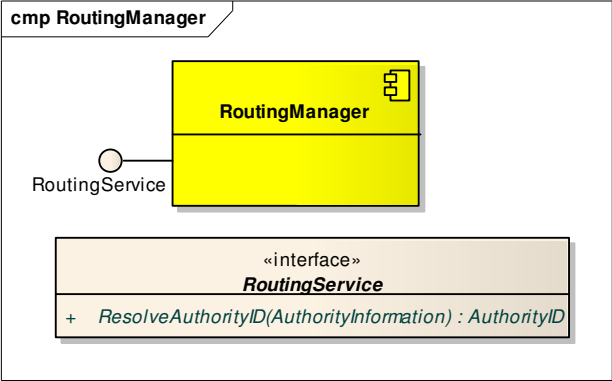
	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
JWG 3.8/3.9: Joint Working Group		Date: 14/05/2010



**Figure 43 - Document Provider WorkflowManager-TransformationManager Interaction Use (OUT\_WM\_TM\_IU)**


### 5.9 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.



**Figure 44 RoutingManager component**

**ResolveAuthorityID (AuthorityInformation) : AuthorityID**

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

<b>Textual description of operation</b>	
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.	
<b>Input parameters</b>	<b>AuthorityInformation</b> Not specified in which way authority information is coded.
<b>Output parameters</b>	<b>AuthorityID</b> OID which clearly references the inbound gateway that will be requested.
<b>Notes</b>	<TODO: Check specification of OID resolving, not found yet>

## 5.10 Configuration And Monitoring Manager

As one of its subcomponents, ConfigurationAndMonitoringManager should include an Abuse Detection System. This subcomponent should be responsible for analyzing the audit trail and, based on a configurable rule set, prevent possible abuses (such as excessive requests issued from a HCP or a patient is queried from more than one country at a time).

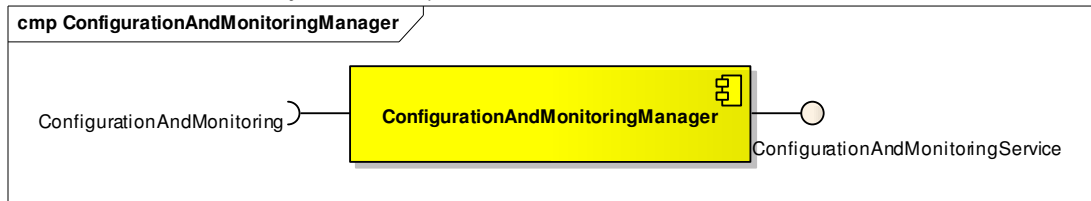



Figure 45 ConfigurationAndMonitoringManager component

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

## 5.11 NationalConnector

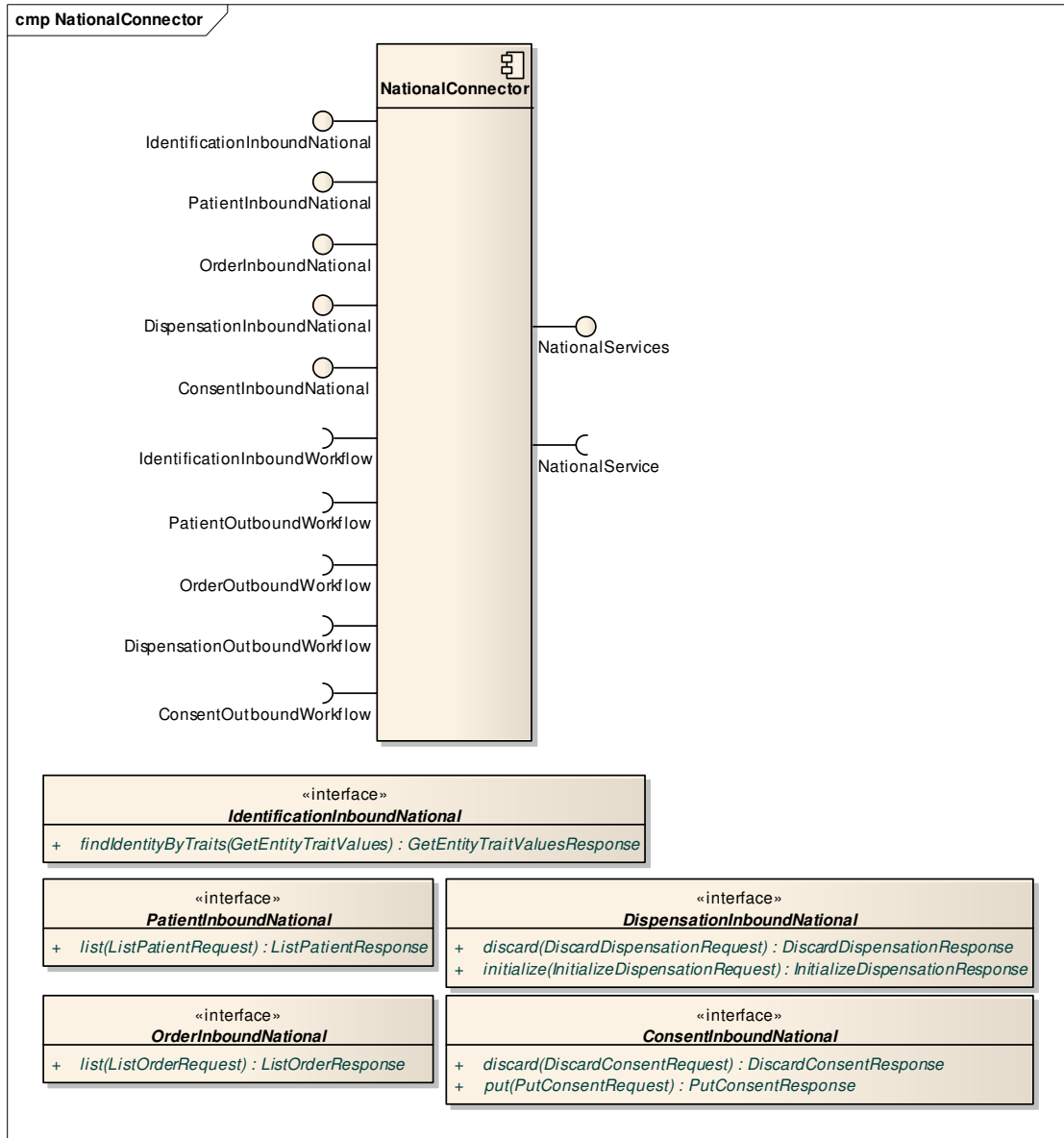



Figure 46 NationalConnector component

The NationalConnector is a component that is developed by MSs and is responsible for connecting the NCP to the national infrastructure of the MS. In order to ensure that the commonly developed components can interoperate with the NCP-in-the-box, interfaces the NationalConnectors exposes to the WorkflowManager should be kept consistent across all individual implementations.

Interfaces of the NationalConnector exposed to the national infrastructure are defined by a MS and therefore are not described in the document.



	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

## 6 Proposals for implementation strategies for Components in Common and Components Non in Common

Chapter 3 has provided the overall architecture and the generic description of NCP components, while Chapter 5 has analyzed in deeper detail the component High Level Specification.

In this chapter we present a rough estimate of the effort to implement NCP-A, NCP-B, and the Front-end and some hypotheses on possible implementation strategies.

### 6.1 NCP Implementation Strategy

The HLDD document has provided the specification to implement the NCP as a Transparent Box.

The choice of every MS to adopt or not the possibility of exploiting common components and, as a consequence of the common agreement, the development in common of such modules, should be also base on advantages and disadvantages of adopting an NCP-In-A-Transparent-Box.

The possible **Advantages** might be:


- Development done (almost) only once
- Members of the Industry Team may candidate to develop single components
- Easier to guarantee compliance with security, legal requirements and FWA
- Simplified integration
- Simplified testing procedures (always in line with Overall Testing Strategy and IHE)
- Simplified deployment procedures
- Simplified evaluation procedure

On the other side, possible **Disadvantages** might be:

- Lower possibility to compare different technical solution
- Less customization to MS specific needs
- Need to manage a European procurement process (other solutions...)
- Need to manage quite a complex development & testing process
- Need to synchronize Common part and MS part development

If it is decided not to develop any NCP components in common, leaving the full implementation to MS, avoiding need for synchronization, the possible pros and Cons should be considered:

- Pros:
  - Apparently shorter development time
  - More straightforward development

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

- Cons:
  - Higher risk to be mitigated by specifically careful testing
  - No optimization and reuse

The Implementation of the NCP and or the development of the Components in common could be done by the Beneficiaries, or by Suppliers selected with an Open Call for Tender.

Call for Invitation / Call for Tender should fulfill the rules stated by:

- DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts

However, considering the nature of epSOS Pilot as a demonstrator of a R&D Project, not a standard service, the Procurement Departments might evaluate the applicability of the Article 31

- **Cases justifying use of the negotiated procedure without publication of a contract notice:**

Contracting authorities may award public contracts by a negotiated procedure without prior publication of a contract notice in the following cases:

...

- (2) for public supply contracts
  - (a) when the products involved are manufactured purely for the purpose of research, experimentation, study or development; this provision does not extend to quantity production to establish commercial viability or to recover research and development costs;

If Article 31 is applied, the possibility of performing Negotiated Procedures with Members of the epSOS Industry Team could be taken in consideration.

The respect of the transparency is assured by the fact that epSOS Contract was assigned after a Public Tender.

The existence of the Industry Team is publicly communicated on the Portal.


The existence of rules and procedures according to which ANY interested Entity can present an application to enter into the epSOS Industry Team is publicly available.

Such rules and procedures have been applied to accept members in the epSOS Industry Team.

MSs, PEB and PSB, while defining the procedures to be followed to implement the epSOS NCP, choosing among the alternatives that developments are done by Beneficiaries or they are done Suppliers.

The pros and cons of these alternatives might be summarized as follows:

- Developments by Beneficiaries
  - Pros:
    - Exploit allocated resources
    - Exploit existing experience
    - Exploit existing solutions
    - Easier management of Change Request

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name: NCP - HLDD
		Version: 1.0
	JWG 3.8/3.9: Joint Working Group	Date: 14/05/2010

- Cons:
  - Need to assure industrial level development
  - Need to check availability of skilled resources
  - Existing solutions must be made fully available to other beneficiaries
  - No real contractual leverage to get deadlines respected
  - Maintenance is not assured
- Developments by Suppliers:
  - Pros:
    - Exploitation of existing commercial solutions
    - Contractual customer/suppliers relationship with clauses to be respected
    - Industrial/professional level of solutions
    - Possibility to negotiate price
    - Maintenance has to be inserted in the contract
  - Cons:
    - Can IT members participate to any Call for tender, having developed specs?
    - Can IT members be invited to a Negotiated procedures, applying Article 31?
    - Necessity to adapt epSOS requirements to exploit existing products
    - Products should be made available also to new beneficiaries
    - The option of “Open Sources” might be rejected by Industry
    - Change request might need contract review


All the considerations, the alternatives, the advantages and disadvantages listed in this chapter, together with planning timing impacts, should be taken into account by PEB / PSB to define the Implementation strategy to be as opted for epSOS Pilot implementation.

## 6.2 Estimation of development effort of NCP-in-a-transparent-box components

### 6.2.1 Estimation baseline assumption

Fraunhofer Institut, ELGA and Tiani-Spirit made a proposal to implement NCP in a Transparent Box and the Country B Front-end portal, including the contribution of several other Industries providing the NCP components.

The proposed implementation, in line with HLDD and the associated effort will be provided in dedicated parts of the Low Level Design Document and of D3.9.1.

	Architecture of the National Contact Point in a Box (NCP-in-a-Transparent-Box)	Document Short name:	NCP - HLDD
		Version:	1.0
	JWG 3.8/3.9: Joint Working Group	Date:	14/05/2010

## 6.3 Further steps towards the Design Specification and Guidelines

This chapter provides indication on components to be specified in detail and actions to be performed.

- Make Low-Level Design (LLD) for specific components, recommended, in order to complete the specifications for the reference implementation performed by Fraunhofer / ELGA / Tiani-Spirit, and for the MSs and Vendors who want to implement NCP and/or the portal from their own. In particular the following elements should be carefully specified:
  - Transformation Manager, including the input XML and the eP, eD, PS, Consent, PDF CDA document schemas, if needed.
  - Terminology Service Access Manager, including the SVS Profile to interface the Central Services
  - Inbound- and outbound- manager parts (not all)
  - Interface (methods and information objects) to national connector
  - Audit manager
  - Service Routing manager
  - Security manager
  - WSDLs & XML schemas for information objects
  - Error Codes on NCP-epsOS level, NCP-national connector level
  - Automatic (Performance) Data Collection
  - Central Services components and interfaces
- Define Technical Rules, Check-lists, Guides & Practicalities descriptions for WP3.8
- Define Testing Methodology and tools to be applied both to Commonly Developed Component and to the National Connectors to allow the overall integration test