EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR HEALTH AND FOOD SAFETY

General Affairs
Information systems

eHealth DSI
Patient Summary and ePrescription

NCPeH Deployment Guide

DOCUMENT VERSION 2.0.0

DATE 28/03/2017

STATUS Release Candidate

Disclaimer	"Release Candidate" versions are provided for evaluation/approval purposes only. Minor updates that benefit the document maturity are expected towards the "Production Release". Responsibility for the information and views set out in this document lies entirely with the authors. Reproduction is authorised provided the source is acknowledged.

COVER AND CONTROL PAGE OF DOCUMENT	
Document old name:	D3.8.2 Final National Pilot Set Up and Deployment Guide
Document name:	NCPeH Deployment Guide
Distribution level*:	PU
Status:	Release Candidate
Author(s): Organization:	eHealth DSI provider EU

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

ABSTRACT
The guidelines are mostly directed at people responsible for setting up the National Contact Points (NCPs) in the deploying countries. The guidelines are referring to the Specifications and reflect the development of the eHealth DSI up until now. In the document you find guidelines on how to handle legal, technical, organisational and practical issues when setting up the NCP and when your system is up and running.

CHANGE HISTORY				
Version	Date	Status Changes	From	Review
V3.0	2013-01-20	Final edit before release	National Board of e-Health	Mie H. Matthiesen
V2.0.0	28/03/2017	Remove all references to epSOS and requirements	eHealth DSI provider	

TABLE OF CONTENTS

1 Executive Summary 5

2 Introduction 5
2.1 Scope and Goal 5
2.2 Structure of the Document 5

3 Technical issues 6
3.1 Functional & Technical content 6
3.2 Architecture of eHealth DSI 6
3.2.1 Overall Structure and Components 7
3.2.2 Interoperability 8
3.2.3 Interfaces 8
3.3 Setting up a NCP 9
3.3.1 Certificates 9
3.3.2 NCP Components in Common 10
3.4 Technical Aspects of eHealth DSI 10
3.4.1 Interconnectivity 10
3.4.2 Patient Identification 11
3.4.3 Patient Consent 11
3.4.4 Health Professional Authentication 11
3.4.5 Semantic Services 12
3.4.6 Patient Summary Services 13
3.4.7 ePrescription/eDispensing Services 13
3.4.8 Platforms 13

4 Legal Issues 14
4.1 eHealth DSI privacy, Security and Information Quality Policies 14
4.1.1 Data protection and confidentiality 14
4.1.2 Information security 14
4.1.3 to semantics 14
4.2 Contractual aspects 14
4.2.1 MultiLateral Agreement 14
4.2.1.1 Forming local variations of the MultiLateral Agreement 14
4.2.1.2 Process for agreeing on local variations MLA 14
4.2.1.3 Signing of MLA 14
4.2.2 Legal Establishment of NCP 14
4.2.3 Legal relationship between NCPs 14
4.2.4 Legal recognition of Point of care and Health care Organisation 14
4.3 Security Aspects 14
4.4 Liability 14

5 Organisational Issues 15
5.1 Establishment of NCP organisation 15
5.1.1 General NCP Organisation 15
5.1.2 Description of Organisational NCP Roles NCP 15
5.1.2.1 Organisational issues stemming from the NCP's functional behaviour 15
5.2 NCP Operating Organisation (Selected Processes) 16
5.2.1 Support Organisation 16
5.2.1.1 Incident Management 16
5.2.1.2 Problem Management 17
5.2.1.3 Change Management 18
5.2.1.4 Service Level Management 19
5.2.1.5 Configuration Management 21
5.2.1.6 Security Management 22
5.3 Security Organisation 22

5.4 Auditing Organisation *23*
5.5 Central Services *23*
5.6 Organising the TestProcedures *25*
5.6.1 Gazelle 25
5.6.2 Simulators 25
5.6.3 Test Data 25
5.6.4 Lab Tests 25
5.6.5 Test of Common Components 25
5.6.6 Test of National Connector within Deploying Country 25
5.6.6.1 Test from/to National Connector from/to NCP 26
5.6.7 Pre-Projectathon 26
5.6.8 Projectathon (PAT) 26
5.6.9 Projectathon on-line 26
5.6.10 Pre-Production Testing (PPT) 26
5.6.11 Regression Testing 27
5.7 NCP Roles *27*
6 Practicalities 29
6.1 Manual processes *29*
6.1.1 How to run the NCPeH in daily use 29
6.1.2 How to handle eHealth DSI at the PoC 30
6.2 Manual regulations to run the NCP *31*
6.2.1 Servers to be used for the NCP – virtual/dedicated 31
6.2.2 Securing the server room and servers 32
6.2.3 Training System administrators and other support staff 32
6.2.4 Nondisclosure agreement for system administrators 32
6.3 Communication Structures within eHealth DSI *33*
6.3.1 NCP as Communication Centre 33
6.3.2 National eHealth DSI Services Coordinator 34
6.4 Semantic Services (MVC and MTC) *34*
6.4.1 Transcoding and Mapping 35
6.4.2 Transcoding and Mapping 36
6.4.3 Semantic safety issues 37
6.4.4 MTC Maintenance 37
7 Glossary 38
8 References 38
Appendix A – Deployment Plan 38

1 Executive Summary

The NCPeH Deployment Guide (or deployment guidelines) is created for people responsible for setting up the National Contact Points (NCPs) in the deploying countries. The guidelines refer to the specifications and reflect the development of the eHealth DSI until their final release.

The guidelines contain information on how to handle legal, technical, organisational and practical issues when setting up the NCP and when national system is already up and running.

2 Introduction

In general, the national side of the NCP is left for the deploying country to handle themselves together with local experts. That's the reason why the guidelines don't present the gap analyses in all countries concerning the relevant existing infrastructures and IT systems which could be used in the deploying countries.
The guidelines focus on the description on how deploying country might set up their NCP.

In order for the guidelines to be useful, the different chapters in the document are directed to the relevant people and hence, written in a language and level of details that is useful for that particular target group.

The guidelines are written in English. If necessary the relevant translations should be provided by the national eHealth DSI team.

2.1 Scope and Goal

The guidelines create a Setup Guide supporting the Competence Centres (CC) and national experts in setting up their National Contact Point (NCP).

In eHealth DSI, the national IT systems are integrated and customised to be able to exchange ePrescriptions and Patient Summaries with other European countries. How this integration and customisation is done differs between the different national systems, depending on the national IT Infrastructure.

The objective of the guidelines is to gather, refer and advise on currently existing:

a) Organisational/Legal/Practical/Evaluation matters
b) Technical matters

2.2 Structure of the Document

The guidelines were prepared according to set off below mentioned rules and methods. The goal was to prepare coherent and useful document, which wouldn't duplicate other specifications.

Set of rules:

1. Find all eHealth DSI requirements related to the section in question.
2. Find the eHealth DSI specifications where these requirements are dealt with.
3. New demands and ways to understanding or working within eHealth DSI should not be proposed by this document *if relevant text is already available* in approved documents. Based on these documents, we should write *short and understandable text and refer to chapters in the approved documents*. Where *no text is available* we should guide and advise deploying countries. It will mostly be relevant in Organisational and Practical chapters.

4. Nevertheless, check if parts of available specifications can be used for Organisational Issues, Practical Issues etc.
5. In the guidelines, refer to the appropriate sections of specifications by name, chapter and page of the eHealth DSI document.
6. Make clear what *requirements* are and what *recommendations* are.
7. Identify missing key points, include them in the guidelines if possible, and make Work.
8. Pure Legal text should be at Legal chapters, Organisational text in Organisational chapters and so on. Exceptions may be needed.

Another goal of the guidelines was to be readable and understandable for people who have not been part of eHealth DSI' development. This might be people who will be part of developing eHealth DSI components for the nation side of the NCP.

3 Technical issues

The technical guidelines must be used as a roadmap to other primary sources, where the information is rightfully described. The following sections (sections in chapter 3) will split the technical guidelines in sensible areas and provide references to the primary source of information on the subject. The information index was created to ensure that information about eHealth DSI are rightly visible. Moreover, the sections can be used as a checklist for the deploying country implementers, for checking their design, planning & post implementation checking.

3.1 Functional & Technical content

See the page on Confluence eHealth DSI Interoperability Specifications.

3.2 Architecture of eHealth DSI

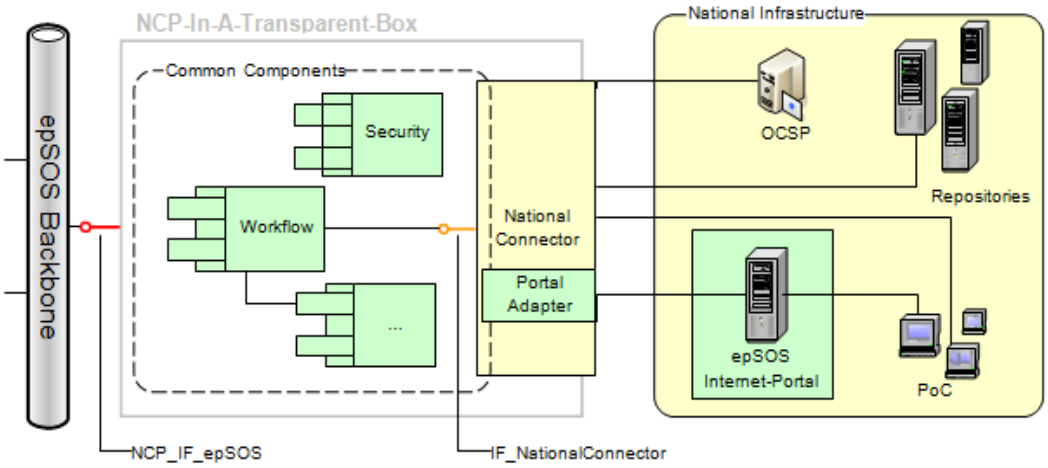


Figure 1: Conceptual Architecture of eHealth DSI NCP Gateway

One of the main objectives of eHealth DSI is to ensure the interoperability between individual NCPs. Chapter 6 of [System Architecture Specification] is dedicated to provide a high-level architectural description of a NCP that should serve as a reference for a detailed specification documents as well as for development planning process.

3.2.1 Overall Structure and Components

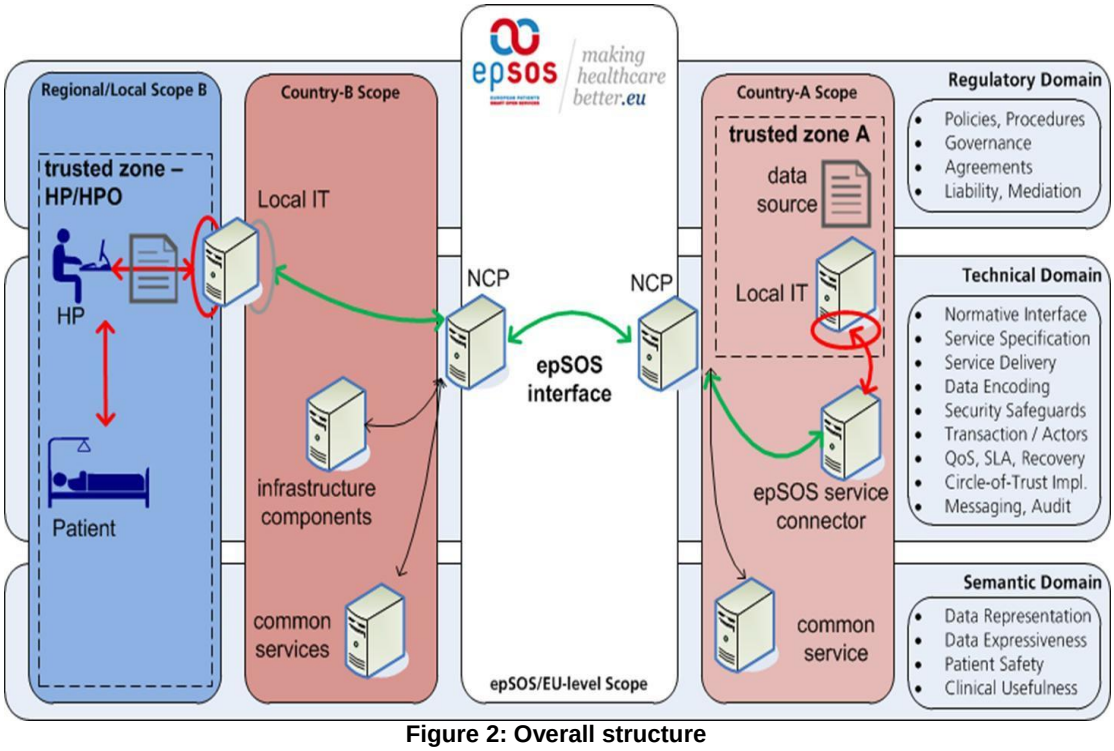


Figure 2: Overall structure

As well as having the role of hosting a set of the technical functionalities and messaging capabilities, the NCP is also home to significant other domains due to the NCP's convenient location at the hand-over point between two or more areal domains. Horizontally, the NCP's provide functionality anchors for the regulatory/organisation domain, the technical domain, as well as the semantic/knowledge representation domain. Vertically, those functional domains are streamlined and harmonised to enable a common service provision & delivery towards the actors of both, country-A and country-B.

SOA paradigm with SOAP chosen for an information exchange was chosen as a basis for NCPs interoperability. Section 6.3 of [System Architecture Specification] provides a technical overview of the eHealth DSI service architecture. The architectural view on the components is given in [System Architecture Specification], section 6.4.

3.2.2 Interoperability

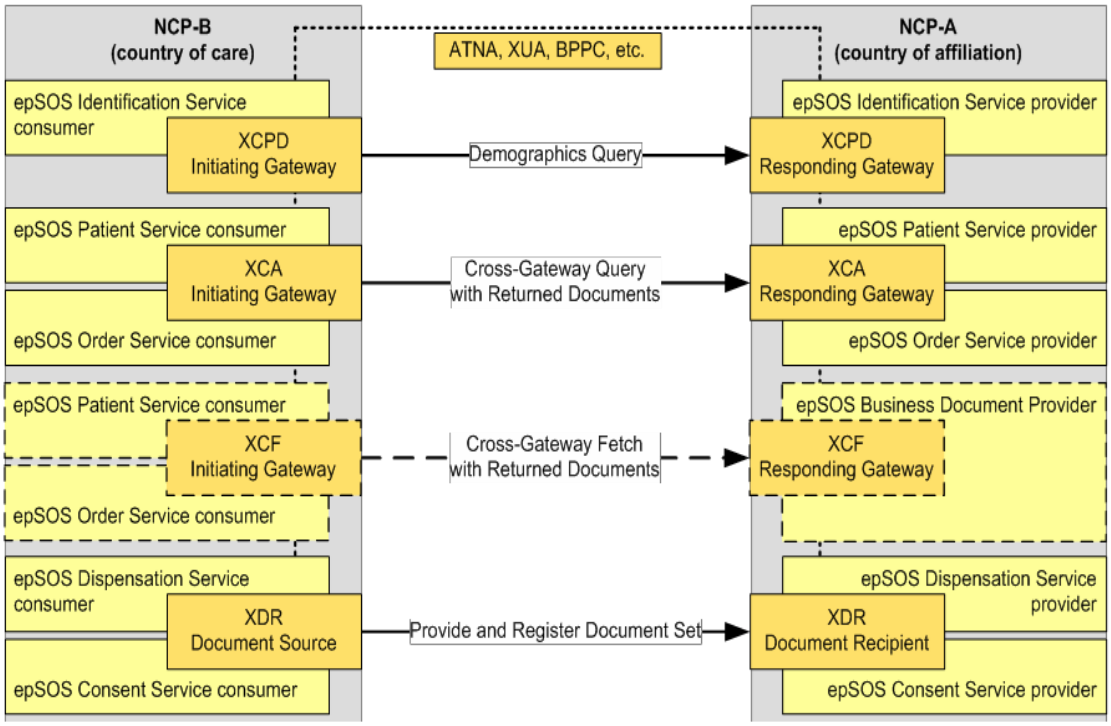


Figure 3: Interoperability

The different aspects of interoperability are summarised in the Interoperability Framework that has been designed as a guide to the standards and protocols that are used to support the interoperability between the deploying countries.

The Interoperability Framework identifies four main categories of interoperability which are legal, organisational, semantic and technical aspects of interoperability. Technical interoperability is achieved with the stipulations in [System Architecture Specification] and [NCPeH Components Specification] regarding standards and interfaces between NCPs.

Traditionally standards are “profiled” before implemented into a production system. This removes flexibility that could otherwise have led to ambiguity regarding the implementation and may help minimising the technical interoperability issues. The comprehensive set of technical profiles that are used within the eHealth DSI specification are elaborated in [NCPeH Components Specification] for the detailed overview of technical interoperability profiles.

3.2.3 Interfaces

The one normative interface in eHealth DSI is the interface of a NCP gateway towards the eHealth DSI backbone (NCP_IF_epSOS, coloured in red in Figure 1). In [System Architecture Specification], the interface is described in the Technology View. It is deduced from the eHealth DSI transactions which are analysed in Business View and Information System View.

The detailed specification of the WebService interface including WSDL and XML Schema can be found in [NCPeH Components Specification].

The other important interface of the NCP gateway is not normative according to the eHealth DSI specification but becomes relevant if a deploying country makes use of the design approach as described in the [NCPeH Architecture Specification]. It is the interface of the national connector towards the “common components” part of the

NCP (IF_NationalConnector, coloured in orange in Figure 1). Aim and conditions of that interface are defined in [NCPeH Architecture Specification].

The detailed specification of the interface IF_NationalConnector can be found in technical specification of the [NCPeH Components Specification].

3.3 Setting up a NCP

This section covers only technical aspects of setting up a NCP. The guidelines on organisational preconditions and recommendations can be found in chapter 5 and 6 and include establishment of NCP organisation described in section 5.1 (Establishment of NCP organisation), definition of NCP key roles described in chapter 5.7 and testing strategy described in chapter 5.6.

It is up to each deploying country to obtain the appropriate hardware and software for the NCP and to perform the ICT installation, however, eHealth DSI requirements on security described in [Requirements and Recommendations] and in [Security Services Specification] must be followed. Some requirements and recommendations on servers for NCP are described in section 6.2 (Manual regulations to run the NCP) and recommendations on operating systems, platforms and libraries are in section 3.4.8 (Platforms and Technical issues). The system must be configured according to eHealth DSI requirements described in [Security Services Specification] and [NCPeH Components Specification].

The NCP components will be provided by deploying country implementer and/or Common component developer along with the installation instructions. These instructions will also include information on how to configure the NCP using the central configurations provided by eHealth DSI. For more details about the central configurations see section 5.2.1.5 (Configuration Management).

After the NCP components have been successfully installed, configured and tested, they need to be connected to the national infrastructure to services for identifications and authentication of patients and health professionals and for obtaining the documents to be transferred to another country (Patient Summary, ePrescription, etc.). Connecting the NCP to the national infrastructure is deploying country responsibility and is out of scope of these guidelines.

3.3.1 Certificates

Each NCP MUST describe its service addresses and certificates in a location table that complies to the eHealth DSI Service Metadata Publisher (SMP) specified in [TSL Profile] section 2 and make this list available to other NCPs via a centrally managed table.

eHealth DSI compliant certificates MUST be Common PKI compatible (see [X.509 Certificate Profiles]).

Key Usages:

Certificate Type	KeyUsage	ExtendedKeyUsage
VPN Client	digitalSignature	opt. "ClientAuth"
VPN Server	keyEncipherment	opt. "ServerAuth"
TLS Client	digitalSignature	opt. "ClientAuth
TLS Server	keyEncipherment	opt. "ServerAuth"
Object Signing	digitalSignature, nonRepudiation	not allowed
OCSP Responder	nonRepudiation	opt. "id-kp-OCSPSigning"

Mandatory Basic Constraint for End-Entity Certificates

"*BasicConstraints*" MUST be included as an extension in the certificate. The extension **MUST** always be designated as critical. The extension **MUST** assume the value FALSE for "ca".

Algorithms and Key Lengths
Algorithms and key lengths must be used in compliance to the following requirements as presented in ECRYPT-II D.SPA.57 (with further profiling by eHealth DSI):

MUST fulfil Level-5 (Legacy Standard 96-bit equiv.)
MUST NOT use Elliptic Curve algorithm without community agreement
MUST NOT use SHA-1
SHOULD use Level-7 (Long Term Protection 128-bit equiv.)
SHOULD use SHA-256

CA Accreditation Requirements
Certificate Authorities **MUST** be registered in the EU Trusted Lists of Certification Service Providers.

3.3.2 NCP Components in Common

The eHealth DSI has proposed a common design specifying common components that can be developed in common. To achieve high interoperability and conformity between the different NCP installations, these common components will be developed for eHealth DSI and the deploying countries. The needed work of designing and specifying the High-Level Design for the components and interfaces is documented in [NCPeH Components Specification].

3.4 Technical Aspects of eHealth DSI

This section contains various important aspects on the technical standard of eHealth DSI. As previously mentioned each section points out to the primary source of information on the relevant aspects. If there is a conflict between eHealth DSI descriptions, the referenced document has to be seen as a primary source of information.

See section 4.1 for list of references eHealth DSI documents/deliverables.

3.4.1 Interconnectivity

The eHealth DSI services fundamentally require the initiation, implementation, maintenance of a common trust establishment between all participating nodes (gateways) that immediately interface eHealth DSI. The organisational trust that is established and secured by a set of MultiLateral Agreement [MLA], policies, and contracts between the eHealth DSI partners must be transposed to the technological foundation of eHealth DSI – eHealth DSI NCP2NCP session.

- See eHealth Network Organisational Framework for eHealth NCP [eHN-OFW]
- See [MLA]
- See [NCPeH Components Specification]
- See [Security Services Specification]

The technological establishment of mutual trust between the trusted nodes (gateways) – referred into within eHealth DSI as trusted node infrastructure or NCP2NCP session – is normatively specified in [NCPeH Components Specification] section 4.1 and IHE ATNA as specified in IHE ITI TF-2a, section 3.19. The concrete security constraints and requirements are elaborated in [Security Services Specification]. Implementation and deployment options are briefly illustrated in [NCPeH Components Specification] in section 3.6.2

- See [NCPeH Components Specification] for the normative specification of the trusted node infrastructure
- See in IHE ITI TF-2a for the detailed specification of the mutual node authentication
- See [Security Services Specification]
- See in [NCPeH Components Specification] for a potential implementation and deployment illustration

3.4.2 Patient Identification

The procedures and processes regarding the patient identification within eHealth DSI are divided into three principal layers:

- the technical processes, identity information container and transport methods as specified in [NCPeH Components Specification] section 5.
- the legal & organisational requirements (including the security safe guards), primarily provided by [Requirements and Recommendations].
- the concrete deployment options as illustrated in [Identity Management Specification] section 5 and the [NCPeH Components Specification], section 3.3.1.

- See [NCPeH Components Specification] for the normative identification transactions, encoding, container, and specific normative interfaces
- See [Identity Management Specification] for the procedural (organisational and legal) definition and requirements
- See [Identity Management Specification] for the concrete set of security safe guards that need to be met
- See [Identity Management Specification] and the [NCPeH Architecture Specification] for potential deployment options

In addition to the technical specification, the legal foundation, and the security safe guards the eHealth DSI specifications also provide a comprehensive set of identification process options and potential process implementation candidates for carrying out the patient identification within the respective deploying country.

- See [Identity Management Specification] for candidate process implementation candidates of patient identification
- See [Identity Management Specification] for a proposed set of identity traits to be used in the identification process
- See [Identity Management Specification] for advice on identification means, such as smart cards or other identity token
- See [Identity Management Specification] for a compilation of the required actors and roles required to identify subjects

3.4.3 Patient Consent

Legal framework and requirements for patient consent will be defined in [MLA].

The technical aspect of exchanging the patient consent is done by a WebService. The architecture for this service is defined in [System Architecture Specification] chapter 6.5.1.5 (Consent Service) and the transactions/profile in [NCPeH Components Specification] chapter 2.6 & 3.6. The exchanged documents giving the patient consent follow the IHE BPPC standard, and are transferred from country B to A.

3.4.4 Health Professional Authentication

Health professional identity data is administered in autonomous systems within national infrastructure. For the eHealth DSI it is assumed that the Healthcare

Professional and HealthCare Professional Organisations that treat the patient can only be unequivocally authenticated by the competent authorities of country B.

The authentication of the Healthcare Professionals is a prerequisite for any eHealth DSI transaction (usually Identification Handshake). The authentication of the Healthcare Professional is done by the identity provider which is part of the national infrastructure and must be separated from the NCP. For more details on identity providers and authenticity levels, see [Security Services Specification] (mainly sections 4.3 and 5.3). The processes for identification and authentication of HP are described in [Identity Management Specification], section 5.3.1 (Identification and authentication of HP).

eHealth DSI country-B implementations may use existing local/national Identity Providers for issuing health professional Identity assertions. The requirements for this case are described in [NCPeH Components Specification], section 4.4.6 (Identity providers) as well as in CP-24 to enable smartcard authentication and Single-SignOn for French health professionals.

The identity ID and its attributes are then communicated among NCPs by means of a normative container structure, the healthcare professional Identity Assertion, as specified in [NCPeH Components Specification], section 5.2 (health professional Identity Assertion).

The establishment and existence as well as the professional acknowledgement of a treatment relationship between a patient and a HP can only be attested within the legal framework of the point of care (PoC). With eHealth DSI health professional authentication and treatment relationship, attestment is therefore performed within the country of care (e. g. by using an existing Identity Provider service of the national infrastructure). The existence of this particular trust relationship may be of significant importance for an access control decision on the PoC and therefore must be communicated towards the eHealth DSI domain. Consequently, NCP-B asserts the correctness of the respective claims and maps them onto a unified syntax and semantics that can be processed by the NCP of country A subsequently. The treatment relationship confirmation is communicated by means of Treatment Relationship Confirmation Assertion described in [NCPeH Components Specification], section 5.3 (Treatment Relationship Confirmation Assertion).

The NCP functionality needed to operate the NCP for the user health professional is implemented in the NCP-B Front-end. The functionality includes health professional authentication, health professional session life-cycle description and TRC session-life cycle and they are described in [NCPeH Architecture Specification].

An overview of the relationship of identity provider to NCP components is described in [NCPeH Architecture Specification], chapter 4 (Exemplary Deployment Composition).

The technical processes, identity information container and transport methods as specified in [NCPeH Components Specification] section 5.

3.4.5 Semantic Services

Semantic services are a cornerstone in the Health DSI providing translation, transcoding, and mapping of clinical documents and information between deploying countries formats. [Semantic Services Specification] defines the methods for semantic translation etc. between deploying countries formats and the eHealth DSI documents.

- See [Master Value Sets catalogue]

- See [System Architecture Specification] and [Semantic Services Specification] for Semantic Services and [Central Reference Terminology Server]
- See [CDA templates] for eHealth DSI semantic components & input format

3.4.6 Patient Summary Services

Patient Summary Service functional requirements and Clinical Document specification are available in the [PS Functional requirements].

Data elements are expressed using HL7 CDA Level 3 Rev. 2 (HL7 CDA here after) with the additional constraints of the HL7 Continuity of Care Document (CCD) and IHE Patient Care Coordination (IHE PCC). The Clinical Document Architecture (CDA) is described in [CDA templates].

Patient Summary lifecycle is described in [System Architecture Specification], chapter 5.5.3, where different states of the process are defined. The details about Patient Summary services interfaces are described in chapter 6.5.1.2, including also implementation recommendations.

NCP Architecture is described in [NCPeH Architecture Specification], this document is a reference for NCP implementers. Section 3.3.2 describes the Patient Service by means of sequence diagrams from both sides, NCP-A and NCP-B.

3.4.7 ePrescription/eDispensing Services

ePrescription Service functional requirements and Clinical Document specification are available in the [eP Functional requirements].

Data elements are expressed using HL7 CDA Level 3 Rev. 2 (HL7 CDA here after) with the additional constraints of the HL7 Continuity of Care Document (CCD) and IHE Patient Care Coordination (IHE PCC). The Clinical Document Architecture (CDA) is described in [CDA templates].

ePrescription lifecycle is described in [System Architecture Specification], chapter 5.5.4, where different states of the process are defined. The details about ePrescription and eDispensing services interfaces are described in chapter 6.5.1.3 and 6.5.1.4, including also implementation recommendations.

NCP Architecture is described in [NCPeH Architecture Specification], this document is a reference for NCP implementers. Section 3.3.3 describes the Order Service by means of sequence diagrams from both sides, NCP-A and NCP-B. Section 3.3.4 describes the Dispensation Notification Service, depicting the sequence diagrams to initiate and discard a dispensation.

3.4.8 Platforms

NCP gateway platforms and operating systems are not normatively specified, and can be seen more as recommendation and intentions, [NCPeH Architecture Specification], chapter 4.3, for design recommendations of platforms & frameworks.

4 Legal Issues

The following matters will be handled by the MLA. Further provisions on deployment guidelines towards legal matters will be **available as soon the MLA is officially released**.

4.1 eHealth DSI privacy, Security and Information Quality Policies

4.1.1 Data protection and confidentiality

4.1.2 Information security

4.1.3 to semantics

4.2 Contractual aspects

4.2.1 MultiLateral Agreement

4.2.1.1 Forming local variations of the MultiLateral Agreement

4.2.1.2 Process for agreeing on local variations MLA

4.2.1.3 Signing of MLA

4.2.2 Legal Establishment of NCP

4.2.3 Legal relationship between NCPs

4.2.4 Legal recognition of Point of care and Health care Organisation

4.3 Security Aspects

4.4 Liability

5 Organisational Issues

Taking in consideration the [eHN-OFW], this chapter provides additional information on organisational arrangements towards NCPeH Set-up.

5.1 Establishment of NCP organisation

5.1.1 General NCP Organisation

Implementing and maintaining the organisation around the NCP requires the deploying country to understand which requirements NCP puts onto it.

This section will identify these requirements and the roles that need to be implemented in the deploying country organisations.

The organisational entities the NCP will influence are:

- operations from service desk to security
- information management department
- audit organisation

Operating the NCP pilot will require the pilot sites to implement the standard package of operating procedures and policies as with any other system:

- The service desk has to be informed and educated about NCP
- Incident and problem management will be required to provide support and services
- The NCP needs to be implemented into national change management
- SLA has to be managed and implemented
- All security related requirements need to be handled on the national level

Information about NCP has to be incorporated into the information flow in/out of the above organisations.

More details on these issues are provided in this chapter.

5.1.2 Description of Organisational NCP Roles NCP

Organisational guidelines are needed to support those responsible for implementing and maintaining the NCP. Examples of such organisational measures can be: procedures (e.g. changes in the organisation) or policies (e.g. specifying responsibilities in agreements and contracts with other parties). The latter case typically applies to the party responsible for implementing and maintaining the national infrastructure.

5.1.2.1 Organisational issues stemming from the NCP's functional behaviour

Functional requirements on the NCP lead to organisational measures. The primary function of a NCP is to support the eHealth DSI use, both as a provider (role NCP-A) and as consumer (role NCP-B); except when NCP-B provides the eDispensation to NCP-A (as a notification). To this end the NCP is to be connected to two infrastructures: First, it is to be legally connected to its deploying country's national eHealth infrastructure. Second, it is to be connected to the other eHealth DSI countries in the circle of trust.

The NCP must have a mandate from the national organisation to access the medical information (also identification & authorisation) of patients (role NCP-A). As NCP-B, the NCP must have a mandate from the national organisation to use the national

infrastructure for authentication and authorisation of healthcare professionals and identification of patient process.

Necessary adaptation, now and in the future, in the national infrastructure as a result of supporting eHealth DSI must be specified in agreements between eHealth DSI and the deploying country. Conversely, future adaptations in the national infrastructure are bound to occur as well. This must be taken into account in the NCP: its connection to the national infrastructure should be checked to see what the effect of local adaptations to the national infrastructure is.

The NCP must be connected to the eHealth DSI infrastructure: The NCP is part of a "federation" (called the eHealth DSI circle of trust). PKI credentials (keys and certificates), used to technically implement the circle of trust, must be protected by technical and organisational measures. Procedures for requesting new credentials in case the current credentials are compromised or in case of failure should be setup with the certificate authority (CA).

5.2 NCP Operating Organisation (Selected Processes)

This chapter describes the organisational setup and procedures within these for operating the NCP. ITIL[1] has been used as framework for the following sections. The selected service and support processes have been deemed minimal requirement for operating the NCPs in a coherent way.

It is for to the deploying country to decide the actual implemented operating management framework, as long as the described functions are established and implemented for cooperation between deploying countries.

The chapter is targeted towards service, support and security management and staff.

5.2.1 Support Organisation

Before entering the system operation each deploying country must have the own national Support Organization set up.

Also the eHealth DSI Central Service Desk for managing the Incidents, Problems and Changes should be acquainted and the interface between National and Central Service desk should arranged.

5.2.1.1 Incident Management

Purpose

All deploying countries must have Incident Management in place for the eHealth DSI. Incident Management is part of the organisation around the NCP or the country. As part of the Incident Management system, the deploying country must have a service desk function. This service desk function will differ from country to country.

Incidents can be technical, organisational or practical.

Incident Management is important for the individual deploying country operations organisation of eHealth DSI in the country itself (country A), as well as other eHealth DSI countries (country B) should be able to contact the deploying country in case of technical or organisational problems in running eHealth DSI.

[1] "ITIL® is the only consistent and comprehensive documentation of best practice for IT Service Management. [...] ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT. ITIL has been developed in recognition of organisations' growing dependency on IT and embodies best practices for IT Service Management." (https://www.axelos.com/best-practice-solutions/itil).

Incident Management aims to restore normal service operation as quickly as possible and minimise the adverse effect on business operations, thus ensuring that the best possible levels of service-quality and -availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits. An 'Incident' is any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service.

Primary functions of the Service Desk include:

- Incident control: life-cycle management of all service requests
- Communication: keeping the customer informed of progress and advising on workarounds

Approach

For operating the eHealth DSI, each deploying country must have the following functions in place organised as a part of the NCP in the country:

- Single point of contact (which are the NSCs) (on national level)
- Single point of entry
- Single point of exit

Deploying countries can organise their Incident Management and Service Desk as it is best fitted into the IT- operation organisation of the deploying country. It could be as part of operating the infrastructure of the country or as a self-contained unit.

Contact information (telephone no. and email addresses) of the NCP Service Desk for each deploying country should be provided.

The contact provided above will serve as the single interface between the deploying country Service Desk and eHealth DSI Service Desk where incidents cannot be resolved nationally and need to be raised to the eHealth DSI level.

5.2.1.2 Problem Management

Purpose

Problem Management aims to resolve the root causes of incidents and thus to minimise the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. A 'problem' is an unknown underlying cause of one or more incidents, and a 'known error' is a problem that is successfully diagnosed and for which either a work around or a permanent resolution has been identified.

Problems and known errors are defined as follows.

Problem management differs from *incident management*. The principal purpose of *problem management* is to find and resolve the root cause of a problem and prevention of incidents; the purpose *of incident management* is to return the service to normal level as soon as possible, with smallest possible business impact.

Approach

eHealth DSI deploying country must have organised ways to solve problems in operating the eHealth DSI. It is here called Problem Management but deploying country might have other names for such functions.

For eHealth DSI purposes the Problem Management should be part of running the NCP as a technical, organisational and practical entity, but eHealth DSI problems to be solved in a country can of course also involve the infrastructure of the country and

the PoC.

Deploying country Problem Management will interface with eHealth DSI Problem Management where problems are identified that cannot be resolved at the nationally and need to be raised to eHealth DSI level.

5.2.1.3 Change Management

Purpose

Change Management aims to ensure that standardised methods and procedures are used for efficient handling of all changes in the technical setup, in the organisational setup or in practical matters in a deploying country.

A change is “an event that results in a new status of one or more configuration items” which is approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure.

The main aims of Change Management include:

- Minimal disruption of services
- Reduction in back-out activities
- Economic utilisation of resources involved in the change

Approach

eHealth DSI founded the Change management structure: the Change manager (ChM) who coordinates the change lifecycle and Change Advisory Board (CAB) which is the body that decides over the proposals related to the change and the structure of the Change management.

eHealth DSI Change management is formalized in the Master document that forms the Annex to Project Management Handbook.

The changes escalated to the central level must be recorded under a ”change” category and follow the approved general lifecycle or in case of certain specific changes follow the predefined workflow model (defined for 4 changes: software-patch, specification, MVC and adding a new deploying country/service).

The Change management also defines the change categories which covers complexity and gravity. Low category changes can be accompanied by direct decision by Change manager without a need to involve CAB.

Each deploying country must have a documented process of implementing changes of technical, organisational and practical kinds. The change process must include proper planning and ensure that sufficient information has been disseminated in the deploying country and to other eHealth DSI deploying country piloting the eHealth DSI services.

Deploying countries making changes in their processes or in their systems must inform other countries about such changes either by mail-communications or by the eHealth DSI Change Manager.
If changes involve systems or processes in other countries it must be decided in a CAB. Such changes should be avoided, but they can be necessary to get the technical solutions to run without serious errors. Legal changes in a country can also impose changes in the eHealth DSI - processes which also involve other countries and have to be handled in a CAB.

5.2.1.4 Service Level Management

The objectives of the eHealth DSI Service Level Management Process are:

- **To list the eHealth DSI Service Levels defined by the Consortium**. The deploying countries are responsible for delivering a particular service within the agreed service levels.
- **To report on deploying Country Service Levels**. The deploying countries are responsible for providing a periodic report on their achieved service levels, their on-going measures for service improvement and any exceptional events.

eHealth DSI Service Level Agreements (SLA)

The SLA describes the service level targets. Service Levels are defined by the Consortium so that it provides a unified Service Level to the users.

SLA is defined for the following services delivered by the deploying country:

- eHealth DSI Systems (eDispensing, ePrescription and Patient Summary)
- Service Desk
- eHealth DSI Systems SLA

Availability:

Availability is the property of being accessible and usable upon demand by an authorised entity (ISO 7498-2:1998). Availability is usually expressed as a percentage of uptime in a given period, presuming that the system is required to operate continuously. If a user cannot access the system, it is said to be unavailable. Generally, the term downtime is used to refer to periods when a system is unavailable.

The eHealth DSI System availability level must be at least 95% per month, 7 days a week from 7.00 am to 8.00 pm, corresponding to downtime between 19,5 and 39 hours per month (30 days).

The availability level is determined on a service level on the NCP of the given deploying country from the point of view of another NCP. In other words, the NCP service of a deploying country has to be available for service requests from other NCPs minimum 95% of the time in the given time period. In clustered setups availability is measured on the entire cluster rather than individual cluster nodes.

Network components outside of the NCP infrastructure are not included in availability measurements.

Since eHealth DSI Services are in an early stage of deployment a higher availability level is not required. The financial investment level between 95% availability (from 7.00 am to 8.00 pm) and 99% availability (24 hours/day) is very high. On the other hand, a lower availability than 95% is not recommendable as the available uptime for the whole eHealth DSI system in worst case then will be less than 60%. This figure will be even lower when the differences in time zones in Europe are taken into consideration.

Monthly calculation:

- 100% of unplanned downtime (application, middleware, operating system failures, etc.) are included in unavailability calculations.
- 50% of planned downtime (maintenance, systems configuration changes, etc.) are included in unavailability calculations.
- Calculation is done on the 7.00 am to 8.00 pm period.

Wherever possible, planned downtime should be performed outside the 7.00 am to

8.00 pm period, and to a common eHealth DSI downtime calendar.

Integrity:
Full integrity of data and applications must be guaranteed by all the systems participating in the eHealth DSI service delivery. Data and systems must be protected against technical or applicative modifications, whether they are incidental or malicious. It must be proved that the transmitted data has not been damaged, reduced or altered. Each serious event will be detected as soon as possible and deploying countries will guarantee their ability to come back to a previous normal situation without any loss and/or distortion of information.

The eHealth DSI System integrity level must be appropriate.

Confidentiality:
Whenever identifiable medical data is communicated, stored or processed, the confidentiality of the data must be guaranteed by all the systems participating in the eHealth DSI service delivery. All communication of identifiable data between the eHealth DSI partners must be performed in a way that prohibits any unwanted disclosure of medical data to any third party. Furthermore, all the systems participating in the eHealth DSI service delivery must assure that any data access is possible only via safeguarded, well-defined interfaces.

An unwanted or unlawful disclosure to an unauthorised party must be prohibited at all times.

The eHealth DSI System confidentiality level must be 100%.

Traceability:
Any data access or attempt to access medical data through the eHealth DSI services must be accountable and traceable (throughout the pilot period) e.g. by logging of “who” accessed, “which” medical data from “where” at “what” time under “whose” authority.

Once all audit data is available, a supervising authority must be able to fully recover and reconstruct an access attempt and access path in order to verify its regulatory compliance. The collected data must be available and suitable for scheduled and unscheduled security audits.

All data gathered by the audit services may contain identifiable personal data, and hence must be protected accordingly. Furthermore, since the audit trail may be considered as evidence/proof in potential investigations, all protocols must be fully safeguarded in terms of integrity and confidentiality. Access to the audit trail must be restricted and only be granted to authorised persons with concrete access necessities within eHealth DSI.

The audit services of the eHealth DSI services should collect a pre-defined set of operational data in order to provide an adequate quality- and capacity- assessment. These protocols must only be used for continuous service delivery and/or service improvement, and must not leave the eHealth DSI context.

The eHealth DSI System traceability level must be 100%.

Response Time:
The response time considered here is the response time perceived by the user between the instant at which he makes a request and the time it takes to receive a response.

The eHealth DSI functional specifications do not ask for response time SLA. It is very difficult to agree on an end-to-end response time SLA, as multiple systems are used in the Patient Summary and ePrescription Services.

It must be noted, however that the eHealth DSI functional specifications make the following recommendation: “Shall be deemed an acceptable response time to load information of less than 10 seconds”. If we want to achieve this objective, we recommend that each system does not exceed 5 seconds of response time for 95% of the requests.

Service Desk SLA
The eHealth DSI Consortium has defined only 3 SLA parameters for deploying country’s Service Desks. These SLA are related to performance but not to efficiency. It is up to each deploying country to define its own level of efficiency.

Abandonment Rate: Percentage of calls abandoned while waiting to be answered.
→ **The Abandonment Rate must be < 10%.**

Time Service Factor: Percentage of calls answered within a definite timeframe.
→ **The Time Service Factor must be > 80% of calls answered in 30 seconds or less (also automatic telephone queues).**

First Call Resolution: Percentage of incoming calls that can be resolved without the use of a call-back or without having the caller calls back the service desk to finish resolving the case.
→ **The First Call Resolution must be > 80%.**

Report on Deploying Country Service Levels
It is the responsibility of each deploying country to provide (publish) a periodic report on their achieved service levels, their on-going measures for service improvement and any exceptional event.

5.2.1.5 Configuration Management

Configuration management holds controls and issues information on all configuration items (CIs) and their components necessary for installing and operating an IT system. It covers the identification, recording and reporting of its components with their versions, constituent components and relationships. CIs under the control of Configuration Management include hardware, software and all associated documentation.

This chapter is important for the deploying country and is therefore included in the guidelines. However, final decisions for the central services, which influence this chapter, have not been taken.

Scope in eHealth DSI
The eHOMB concluded that some central services including the management and provision of specific data will be implemented in eHealth DSI as a service to the deploying countries, to be hosted by a volunteering beneficiary. eHealth DSI is in the process of specifying the requirements towards these services and publishing them for reference.

Semantic operability in eHealth DSI is based on a specific terminology developed for the purposes of the project and provided for usage to all participating deploying countries. A central service eCRTS will manage this terminology with the support of the deploying countries and make it available to each NCP. The functionalities

offered by the service will be described in [Central Reference Terminology Server] along with the technical details on architecture and interfaces to be used.

A central service Configuration Repository Manager will control and provide specific data to the NCPs located in the deploying country thus facilitating the interoperability of all NCPs during their operation. The functionalities offered by the service will be described in [TSL Profile] along with the technical details on architecture and interfaces to be used.

While the above services will support the NCP operation with some centrally managed data, it lies in the responsibility of each deploying country to ensure that their NCP is interoperable with all other NCPs, thus assuming alignment with their configuration.

Technical Realisation
Configuration data required for the NCPs' successful interoperability with partners during the pilot operation include static location tables as described in [System Architecture Specification], [NCPeH Architecture Specification] which will be employed for service discovery and location. Therefore, according [NCPeH Components Specification] chapter 2.1.4, each NCP MUST provide its service addresses and certificates in a centrally managed location table, at the same time each NCP MUST hold a copy of the other NCPs' location tables as part of its internal configuration. This way the NCP assumes responsibility for holding the updated location table locally. The eHealth DSI Configuration Repository Manager assumes responsibility for providing the compiled location table to the NCP via a defined interface as referenced above.

5.2.1.6 Security Management

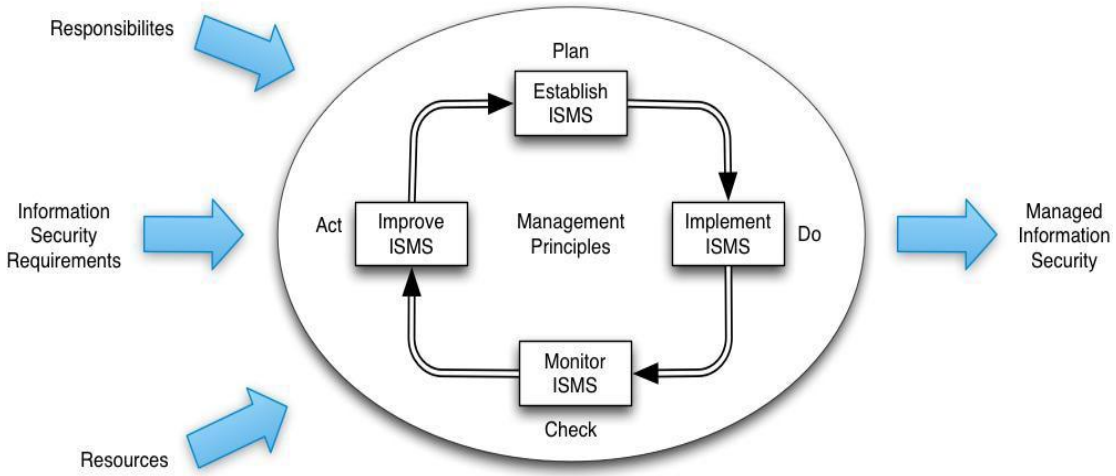
Please refer to chapter 5.3

5.3 Security Organisation

The purpose of security management is to fulfil security requirements in a consistent way open to scrutiny. We are using the terminology and structure of ISO 27001 as the current best practice to describe how information security is to be managed in eHealth DSI. However, NCPs are free to adopt different schemes and standards.

General requirements
"*The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS*[2] *within the context of the organization's overall business activities and the risks it faces. The process used is based on the PDCA model shown below.*" [ISO27001/4.1]

[2] ISMS: Information Security Managed System



Establishing an ISMS
A large portion of the work needed to establish an ISMS is provided by eHealth DSI.

The creation of the SOA (statement of applicability), which handles each single security control, is the main document that defines the safeguards to be implemented. It is:

- An explanation of how the organization complies with them
- An explanation and justification of any deviations from them

5.4 Auditing Organisation

This chapter is an informative chapter as final decisions on auditing has not yet been taken. However, it is an important chapter for the deploying countries as they need to prepare for auditing.

The chapter is in general referring to the security chapter 5.3. All security auditing must be related to the security policy and the security baseline documents. It should be noticed that auditing is concerning technical, clinical, physical and organisational processes in the deploying country.

As known for now, the auditing will be organised as self-assessment by the deploying country. This means that the deploying country must follow certain rules for their auditing processes:

1. Deploying country should appoint one or more skilled auditors and form an auditor structure.
2. Deploying country will write a report stating which audits have been carried out in the country and if all required security measures in the baseline document have been met (the formal structure of the report will be an eHealth DSI checklist).
3. First auditing must be performed according to the Readiness Assessment and Go Live procedures defined.
4. Operational audits (after Going live) should occur as described in the Audit Framework.

5.5 Central Services

The Central Services are described in [Central Reference Terminology Server] and in [TSL Profile] in which the Service Level Agreement has also been agreed upon. In particular:

Chapter 5.1 describes Central Service Goal and makes proposal on associated responsibilities.
Chapter 5.2 describes functions and structures of Configuration Repository

Manager.
Chapter 5.3 defines eHealth DSI Central Reference Terminology Service.

The eHealth DSI NCP-In-A-Box is a machine that [Security Services Specification] classifies as *Secure Node*: no administration access to the machine is allowed. Whenever a configuration changes, an audit trail must be sent to the audit record repository. For this reason, the CCD team defined and developed the following utility applications:

Configuration Manager a client library that reads the *epsos.properties* file containing the configuration information fetched from the central services and the *TSL Synchronizer* that fetches the NSL from the central services.

SyncApp a cronjob that each country shall implement according to their system and network capability in order to exchange xml configuration files between the secure node and the underlying network.

The NCP configuration items are pulled from two sources: A local NCP repository and the eHealth DSI Central Service (eHealth DSI-CS).

Each country must have prepared the following items:

Common items published on the eHealth DSI-CS, such as:

a) The OID of the following codes: XDS_DOMAIN, PI_DOMAIN, HCID, REPID
b) A NSL file, created and signed using the TSLEditor and sent in the DropArea of the central service for the local country
c) Supported identity traits
d) IP Address of the machine that will run the NCP
e) Identity Provider NameID Value

Local items published at some country-specific location, such as:

a) The description of each OID for the remote countries (i.e. in order to link the OID to a display name for the Portal B, it_IT <-> Italy XDS Domain
b) Private Keys following the X509 certificate layout of the [NCPeH Components Specification]
c) An SNMP collector for the configuration manager
d) An *epsos.properties* file already preconfigured for the local NCP (e.g. CountryCode, CentralServices, NslDropZone, NslRunningZone, CoT.CountryCodes, LanguageCodes)
e) A Role Mapping file
f) A PoC Registration file
g) Hostname of the machine (as output of the unix command /bin/hostname)
    - URL of the national infrastructure, for the following services: XCPD Responding Gateway, XCA Responding Gateway, XCA Initiating Gateway, XDS Registry, XDS Repository
h) Emergency policy

The Central Service will provide the run time environment where eHealth DSI Central Reference Terminology Repository Service (eCRTS) is installed.

The Terminology Responsible of the deploying country will access to the eCRTS to manage
(translate/approve the MTC).

The *TSL Synchronizer* calls the specific webservice of the Central service to download the extracted MTC into the Local Terminology Repository.

5.6 Organising the TestProcedures

Before a deploying country can participate in eHealth DSI Operation some test steps, which are described in this chapter, have to be fulfilled (further information can be found in [Test Framework]).

eHealth DSI will provide test cases and simulators based on IHE-Europe test tool (Gazelle). With Gazelle all functional requirement and use cases of eHealth DSI can be tested.

5.6.1 Gazelle

Gazelle was developed by IHE Europe and includes following:

- Test Cases, described as a Storyboard, to run tests step by step
- Simulators for test step by step
- Simulator for NCP A
- Simulator for NCP
- Simulator for end-2-end tests
  - For Patient Summary
  - For ePrescription
  - For eDispensation

In addition, an on-line questionnaire is provided to health professionals to report their experience and feedback during the end-2-end functional testing, performed during Projectathon (PAT) and Pre-Pilot Testing.

5.6.2 Simulators

The Simulators will support the tests to make it easier and to check the outcome.
Test Cases are prepared for step by step tests or complete workflows. (e.g.: Test of Patient Summary)

5.6.3 Test Data

Critical Test Data (CTD): commonly agreed test cases to be used by all deploying countries as reference for Conformance Gate approval. Each deploying country has to generate its own test data based on provided Critical Test Data
Representative Test Data (RTD): they are typical documents from the deploying country either produced by experts or derived from real documents, carefully anonymised. The goal is to exchange a large number of test data to detect as many issues as possible, in order to increase patient safety.

CTD and RTD should be uploaded to Gazelle (http://gazelle.ihe.net/?q=elfinder**)**.

5.6.4 Lab Tests

These tests are the first steps in order of the tests and have to be run within the deploying country. Target is to run successfully the pre-tests for eHealth DSI Projectathon.
For these tests eHealth DSI will not deliver a simulator – the messages to/from the National Connector to the National Infrastructure have to be monitored.

5.6.5 Test of Common Components

Before the Common Components will be handed over to deploying country, eHealth DSI Solution Provider will test their application with dummy data based under test cases of Gazelle.

5.6.6 Test of National Connector within Deploying Country

Test as Country A
The National Infrastructure has to handle with the National Connector following Use

Cases

- Patient Identification
- Validation of Patient Consent
- Patient Summary: CDA document of Patient Summary
- ePrescription: List of ePrescriptions and CDA document of ePrescription
- eDispensation: received CDA document(s) of eDispensation

Test as Country B

Country B can work either via Portal or National Infrastructure has to handle with the National Connector following Use Cases

- Health professional Authentication
- Patient Identification: Identifier of Patients
- Patient Consent
- Confirmation
- Display of Patient Summary
- Display and Select of ePrescriptions
- Generation and sending eDispensation

5.6.6.1 Test from/to National Connector from/to NCP

These tests will be supported with several simulators developed by IHE Europe which can and should be used from the deploying country. Test for Country B can be done either via Portal or National Infrastructure.

5.6.7 Pre-Projectathon

Conformance testing to be allowed to go to the Projectathon, performed from the deploying country Laboratory toward Gazelle.
For participating in PAT the deploying country has to report that all Gazelle Test Cases were fulfilled depending on the scenarios.
Only deploying countries with positive results can participate at PAT.

5.6.8 Projectathon (PAT)

IHE Connectathon like f2f event to perform Conformance and Interoperability testing. It includes end-to-end functional testing.
NCP-A, either connected to the real or to the emulated National Infrastructure, and NCP-B, possibly connected to the Country B Portal are tested toward Gazelle and among them.
The plan is to have end-2-end tests (National Infrastructure A -> NCP-A -> NCP-B -> National Infrastructure B and vice versa), with the participation of health professional of Country B. PAT allows deploying countries to enter in the Pre-Pilot Testing.

5.6.9 Projectathon on-line

On-line sessions based on Gazelle tests, to allow deploying countries to get approval to go to the PPT. Since PAT is not very frequent and requires a significant organisational and economic effort, it has been decided that, the deploying countries who have participated in a PAT, may perform PAT-on-line either to repeat tests failed at PAT, or to validate new releases or new services.

5.6.10 Pre-Production Testing (PPT)

Pre-Production Testing environment must reproduce the same architecture of the Operation environment, including the connection with the real National Infrastructure and the installation of the CA Certificates compliant to eHealth DSI security Requirements.

Conformance tests are repeated in the PPT environment, including the Workflow

test, to verify the services work in the real piloting environment.

End-to-end functional testing with real infrastructure and virtual data (representative and critical test data). PPT includes the validation of the organisational and legal requirements.
In this phase several deploying countries will test different scenarios with test data and virtual patients on a test environment. This test environment should be available for testing of additional scenarios. Each deploying country should participate in the minimum with one pilot.

Although the PPT is a continuous activity for quality improvement and system/service functional assessment, test slots will be defined. During these test slots, the verification of Conformance Gate 2 satisfaction will be performed.

5.6.11 Regression Testing

Regression test is performed in the Operation Environment, to verify if what was tested in PPT behaves in the same expected way.

Tests are limited to the verification of the capability to establish the VPN, to check no error is generated while retrieving documents from all the other deploying countries and requesting to the Health Professionals to perform a functional end-2-end testing recalling a document (PS and/or eP from all the other deploying countries).

Regression test is also performed in PPT, when a new patch is released.

5.7 NCP Roles

Below is a list of important roles related to eHealth DSI Services. These roles are legal, organisational and practical. The list might not be exhaustive and may vary from deploying country to deploying country.

Role	Description
Change manager	A person-role, but the role can be shared.
Citizens	Citizens are individuals in deploying country who can be patients, relatives of patients, carers or persons who may need to have access to healthcare in the future. At its simplest, citizens are represented as the total population of a deploying country.
Configuration manager	A person-role, but the role can be shared.
Data controller	Is here understood as a term from REGULATION 2016/679, 27 April 2016. Not a person-role, but a legal person (entity) controlling personal data.
Data processor	Is here understood as a term from REGULATION 2016/679, 27 April 2016. Not a person-role, but a legal person (entity) processing data on behalf of the Data Controller.

European Commission	The Commission's job is to represent the common European interest to all the EU countries. To allow it to play its role as 'guardian of the treaties' and defender of the general interest. The Commission has the right of initiative in the law making process. The Commission is also responsible for putting the EU's common policies into practice and manage the EU's budget and programmes. eHealth DSI has been institutionalised by the Commission. eHealth DSI is referring to the Commission as well as the deploying country. The Commission is reviewing eHealth DSI as the Commission is a financial contributor to eHealth DSI.
Evaluation	Person responsible for evaluation of eHealth DSI services.
Health Professional	A doctor of medicine or a nurse responsible for general care or a dental practitioner or a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC. This means that a Healthcare Professional is a person who delivers healthcare or care products professionally to any individual in need of healthcare services, in order to prevent, relieve or treat a medical problem.
Central Services Administrator	Person responsible for technical support to the deploying country terminology team (the deploying country end users) in their creation of the deploying country's terminology content.
Incident manager	A person-role, but the role can be shared.
Legal responsible person	Legal expert representing deploying country and responsible for legal activities in deploying country concerning Pilot preparations. Assure progress in legal pilot preparations and provide reporting on it.
National Authority Beneficiary (NAB)	National health authorities which is represented in eHealth DSI for each deploying country.
National Contact Point (NCP)	Organisation delegated by each deploying country to act as a bidirectional technical, organisational and legal interface between the existing different national functions and infrastructures. The NCP is legally competent to contract with other organisations in order to provide the necessary services which are needed to fulfil the business use cases and support services and processes. The eHealth DSI NCP is identifiable in both the eHealth DSI domain and in its national domain, acts as a communication gateway and establishes a Circle of Trust amongst national Trusted Domains. The eHealth DSI NCP also acts as a mediator as far as the legal and regulatory aspects are concerned. As such an NCP is an active part of the eHealth DSI environment if, and only if, it is compliant to normative eHealth DSI interfaces in terms of structure, behaviour and security policies.
National eHealth DSI Services Coordinator (NSC)	The single point of contact between eHealth DSI and the individual countries regarding all matters concerning run activities.

National eHealth DSI Services Coordinator – Technical Leads (NSC tech.lead)	The national contact person regarding technical implementation of the systems in the deploying countries.
National website administrators	Responsible for national sub-sites under eHDSI and single point of contact regarding website editing.
NCP manager(s) (person(s) or organisation)	The NCP needs managers who are responsible for setting up and running the NCP. This can be person(s) or an organisation which has signed a contract with the NAB and is therefore included in the eHealth DSI circle of trust.
Patient	Any natural person who receives or wishes to receive healthcare in a deploying country.
Pharmacist	Pharmacist working at a pharmacy involved in eHealth DSI.
Pilot site manager	Person responsible for eHealth DSI services at pilot site level.
Problem manager	A person-role, but the role can be shared.
Security Auditor (person or organisation)	Person or organisation in a deploying country taking care of auditing the security for eHealth DSI and eHealth DSI connected ITC systems.
Security manager	A person-role, but the role can be shared.
System administrator	eHealth DSI System administrator is a person (person-role) which has access to alter and correct the system, set up new user accounts. The System administrator must typically have access to all part of the system and by that data in the system. This means root access. Usually responsible for system and network.
Terminology responsible	Person who is responsible for the deploying country's creation of the deploying country's terminology content.
Test manager	If appointed, the test manager should follow the eHealth DSI test strategy to Quality assure the eHealth DSI system with interface to National Infrastructure (Projectathon, Field test etc.)

6 Practicalities

6.1 Manual processes

This chapter cannot be more than advisory, as it is up to the individual deploying country to decide how to run their business processes. Nevertheless, the deploying countries must be able to describe their business processes, so the needed auditing can take place in a transparent way.

6.1.1 How to run the NCPeH in daily use

There are several practical aspects of operating the NCP in daily use:

1. The MultiLateral Agreement
   The MLA should be signed in order to create the trusted circle (see chapter 4).

2. The National Contact Point
   The daily communication between the GPs, Pharmacies, Hospitals and other eHealth DSI entities must be taken care of by the NCP organisation. Communication will be electronically as well as orally communicated. It is

important to establish the communication channels with necessary telephone numbers, addresses etc. for a service desk/service staff, system administrators etc.

3. Managing staff
   A managing structure for all staff involved in the eHealth DSI pilots must be described. Especially, it is important that eHealth DSI system administrators are aware of the security responsibilities in the trusted circles of eHealth DSI, and a sufficient Non-Disclosure Agreement is kept with the eHealth DSI system administrators.

   It is important that management care for initial training. In order to maintain the level of service, further training is necessary along the way.

4. Security matters
   The management of the NCP must be particular aware of the rules described in chapter 5.3 Security organisation and [Security Services Specification].

5. Security Auditing
   Described in Chapter 5.4.

6. Reporting
   A reporting tool in which the deploying countries are to report on pilot implementation status has been created. This way, it is possible to create a consolidated view of the implementation progress within the deploying countries.

7. Monitoring
   Specific KPI are defined for eHealth DSI

8. NCP economy
   Is up to the deploying country.

9. Maintaining the technical set up (Service contracts)
   Needed daily adjustment of server parameters should be done by NCP staff to optimise the operation of the NCP.

   Central services are hosted by European Commission.

10. Updating the Technical set-up.
    Updating the HW, System SW and the eHealth DSI applications must be done according to need and eHealth DSI Frameworks (e.g. Audit, Test, Support). The deploying country NCP management is the responsible for updating the technical set-up and may count on eHealth DSI Solution Provider.

6.1.2 How to handle eHealth DSI at the PoC

In order to handle eHealth DSI at the PoC the following aspects must be dealt with:

1. Training
   The potential users of the eHealth DSI services must have been trained and must be familiar with the pilot services. In the training, they will need to be informed of the aspects mentioned in this chapter.

2. Legal aspects
   The potential users of eHDSI services must be aware of their responsibilities, rights and duties, including processing of patient consent, health

professional authentication, access to the patient information, data protection, liabilities when providing the service to the patient. All PoCs must sign the MLA with the national NCP organisation. By signing this contract, they confirm that they are aware of this.

3. Security
   The security requirements decided in eHealth DSI must be followed. You find a link to them in [Requirements and Recommendations].

4. Safety
   If an error occurs during an eHealth DSI encounter, the Healthcare Professional should follow the normal procedure of the PoC as if eHealth DSI did not exist.

5. Support
   Each country (that has deployed an NCPeH) should set up a service desk where the Healthcare Professional and National citizens can find information and report problems.

6. Information to patients
   Potential patients must be informed about the eHealth DSI project and its services at the PoC and the other locations and the National Communication Guideline. The information needs to include the description and goal of the project and the services.
   Some pre-requisites are needed to be in place in order to handle an eHealth DSI patient:
   - The PoC is legally authorised and registered to use the eHealth DSI service (MLA signed between PoC and NCP-organisation)
   - The dispenser/doctor has been previously trained and is familiar with the pilot service
   - The eHDSI service currently available at the PoC
   - The PoC has information about the pilot service (description of the pilot service, possible outcomes legal aspects, rights and duties) in the different languages to inform the potential eHealth DSI patients
   - A service desk is available (for information purposes and to report problems). This is the responsibility of the NCP-organisation.

In countries participating in eHealth DSI, patient prior consent is the most usual scenario. National communication strategy should make patients aware on their need for action in order to make possible the exchange of clinical data as described in cross-border eHealth Services (Patient Summary and ePrescription).

6.2 Manual regulations to run the NCP

This chapter is partly an advisory chapter and partly there are requirements to be fulfilled. It is a requirement that servers and server rooms are secure and safe, but it is of course up to the deploying country to decide the arrangement for such security.

6.2.1 Servers to be used for the NCP – virtual/dedicated

The servers to be used for NCP can be either dedicated servers or virtual servers, according to decision in the deploying country. The servers can be part of the existing server-environment of the infrastructure in the deploying country or they can be placed in a special set up for eHealth DSI. There can be one or more physical servers with one or more logical servers.

The server set-up must be able to fulfil the agreed eHealth DSI Service Level

Agreement by having the needed redundancy for server capacity, storage capacity, switch capacity, emergency Power Supply etc.

In all cases, the servers must fulfil the demand of security and auditing (see chapter 5.3 and 5.4) and the servers must be according to chapter 3.4.8 Platforms.

6.2.2 Securing the server room and servers

The eHealth DSI Security Team stresses the importance of securing the server rooms and eHealth DSI servers within it. This is caused by the fact that the technical security and accessibility can easily be broken if servers and server rooms are not secure.

6.2.3 Training System administrators and other support staff

Education of and information to system administrators and other staff is a very important and critical factor and will be achieved through a specific introduction session. A training process for support staff can be a series of activities which aim at enabling them to assimilate and develop knowledge, skills, values and understanding a broad range of problems in a way that can analysed and solved. Responsibility of the training lies with the NCP organisation.
The objective of the training process is to provide support staff with sufficient skills in order to support the operation and maintenance of eHealth DSI software, system software and hardware.
Administrator training in general will focus on areas including, but not limited to, system set-up, configuration, system maintenance, administration utilities, security administration and backup/restore of the system.

More specific:

- Knowledge of eHealth DSI architecture
- Knowledge of used standards for communication and interoperability among systems
- Knowledge of support and troubleshooting of systems interfacing Installation, set-up and configuration of eHealth DSI software and hardware System maintenance of eHealth DSI software and hardware
- Security administration of eHealth DSI software and hardware
- Backup/restore of the system and supporting of availability options

How staff is trained is up to the deploying country.

6.2.4 Nondisclosure agreement for system administrators

Generally, NCP system administrators will have no need to see the contents of any data packages passing in the NCP. The administrator will only need to ensure that all authentications are correctly certified and assure the non-repudiation of the data transfer. In some circumstances it may, however, be necessary that, in the course of audit, maintenance or error management the system administrator accesses the content of data packages.

As already described, some deploying countries will not be allowed such access to patient identifiable data. Therefore, they must provide some mechanism whereby data can be duly anonymised or where some duly authorised person can access the system in order to undertake the necessary work.

In many deploying countries, the local legislation will, however, allow the access to patient identifiable data by people other than accredited medical personnel on the basis of contracts conferring a duty of responsibility. If this occurs, such contractual non-disclosure agreements should be foreseen. In accordance with DPA, such

NDAs should include a term which allow the necessary legal action of any person who breaches the NDA.

6.3 Communication Structures within eHealth DSI

It is important that this chapter is read by managers and staff, organising the communication structure in deploying country. In the country, the communication is up to the deploying country, but the communication structure should be described for auditing.

6.3.1 NCP as Communication Centre

The NCP works as a national communication node for several directions.

1. towards eHealth DSI – the communication partner towards eHealth DSI is National eHealth DSI Services Coordinator (NSC). NSC works on one hand as liaison body for transmitting the eHealth DSI requirements and coordination directions, on the other hand as the recipient, processor and distributor of the request of NCP towards eHealth DSI. This communication partnership will last for the whole duration of the Project – both in pre-production testing phase and waves phase.
2. towards other sites – after localisation of MLA and extending of trust domain all the way to the sites (by means of the contracts between NCP – site) each site will have the responsible liaison person communicating with eHealth DSI via NSC (concerning the issues related to coordination of pilot preparation and pilot operation) and with NCP via responsible person mainly for purpose of solving the operational issues (requests receipt and distribution; data quality, integrity and completeness; translations/transcoding).
3. towards the institutions providing the process services (identification; authorisation; audit) if not being integrated in NCP.

Each NCP is recommended to point to experts able to deal with technical, legal, semantic and security issues. List of these experts should be made available within all eHealth DSI trusted domains. These lists are part of the deploying countries' TPM reports.

Means of communication: standard means of communications should be in use (mail, email, and phone). Use of particular means of communication depends on seriousness, urgency and security demand. Communication initiatives and efforts should be recorded in a log book, or any other equal way maintained in the deploying country, for sake of reporting (e.g. towards INEA) and knowledge sharing (e.g. towards other deploying countries).

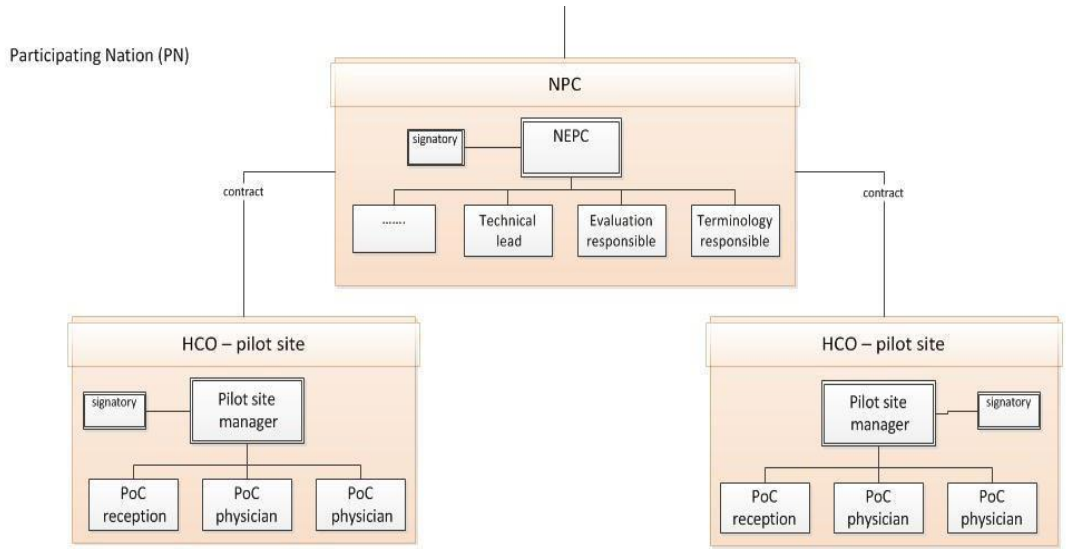


Figure 13: Communication structures

Within the eHealth DSI project environment, the entire communication relevant to pilot operation should go through eHealth DSI Solution Provider to avoid confusions and assure a quality check. eHealth DSI Solution Provider collects the requirements, advice and instructions and transmits them to NCP and vice versa (collects the requests or tasks fulfilled from NCP and distributes them).

eHealth DSI submits to eHOMB the deploying country requests for approval of core milestones and reports back the eHOMB decisions.

6.3.2 National eHealth DSI Services Coordinator

The National eHealth DSI Services Coordinator (NSC) is the role established by eHealth DSI project to ensure the liaison among relevant stakeholders. NSC is a person assigned by NCPeH or eHealth DSI beneficiary. NSC has been nominated by each of deploying countries in eHealth DSI with aim to run eHealth DSI services within their national environment.

6.4 Semantic Services (MVC and MTC)

This chapter deals with the handling of the semantics in the deploying country. It does not concern the technical conversion issues, but only how translation and transcoding should be handled by the deploying country before the start of eHealth DSI, and during the eHealth DSI running period as long as eHealth DSI is in operation.

The chapter should be read by semantic experts and those in deploying country, who are maintaining the semantic structure.

In order to make the semantic flow work in eHealth DSI, the Master Value Sets Catalogue (MVC) has been developed to apply the structured fields in PS, eP and eD. MVC consists of entries with subsets of concepts coming from different international classifications. MVC will secure the semantic interoperability between the countries in eHealth DSI. Thus it would not be necessary to translate everything to every local language in eHealth DSI.

The deploying country will have to use the MVC / MTC (The Master Translation Catalogue) in a service running on NCP in country A before sending PS or eP to country B, transforming, in needed, locally used codes to eHealth DSI codes. [Country A and Country B roles are inverted for the eD scenario].

The Master Translation Catalogue MTC will be used in Country A to transcode – in case – the locally used codes included in the MVC, and in Country B NCP service, when receiving a patient PS, eP or eD in order to translate from English (pivot format) to the local language in country B. [Country A and Country B roles are inverted for the eD scenario].

eHealth DSI provides the pilots with tools for handling the mapping processes on a central server: the eHealth DSI Central Reference Terminology Server (eCRTS). The Single point of contacts will also be offered instruction for two members in each country in using the tool and its functionality. When the different mapping tables are done and qualified they must be downloaded from the central server to the NCP. Each country is responsible for the content in the mapping and translation tables on the central server and when the files are in place on NCP. It is important the individual country attach the right national experts to perform the mapping and translation in the workflows on the central server using the central services.

6.4.1 Transcoding and Mapping

There are two kinds of mappings to be done prior to making the final pilot run:

1. Concept to concept mapping between national used classifications and eHealth DSI MVC.

   Data registration in each country uses national or maybe international concepts and classifications. All these concepts must be mapped to the concepts in MVC before the connection tests of eHealth DSI take place.

   This mapping might be “one to one” or “many to one”: the “one to many” mapping is never allowed. In the “many to one” case the patient registration can use much more codes and this many codes have to be compressed by matching a much less number of codes in MVC. The mapping will lose information, and it is not possible to map back.

National code	Map to epSOS Code
KCJ	54885008
KCJA	54885008
KCJ10	54885008
KCJB	54885008
KCJB00	54885008
KCJB10	54885008
KCJB20	54885008
KCJB30	54885008
KCJB99	54885008
……	……

Figure 14: Mapping example of nationally used codes matching the same eHealth DSI code

   Countries using the same international classification may cooperate and divide the mapping task in order to reduce the work to be done. The mapping has to be done by experts and qualified.

2. Physical fields mapping from national sources to eHealth DSI PS, eP and eD.

   Before the “concept to concept” mapping can take place, the fields in the sources (e.g. national databases from where the data are registered, or documents maintained by the national infrastructure) must be matched to

fields in PS or eP – this is a kind of physical mapping every country has to do on their own. This physical mapping will be used for two purposes:

i. To detect which local or national classification is used in the field
ii. To fill in data in PS or eP when responding a request from a country B

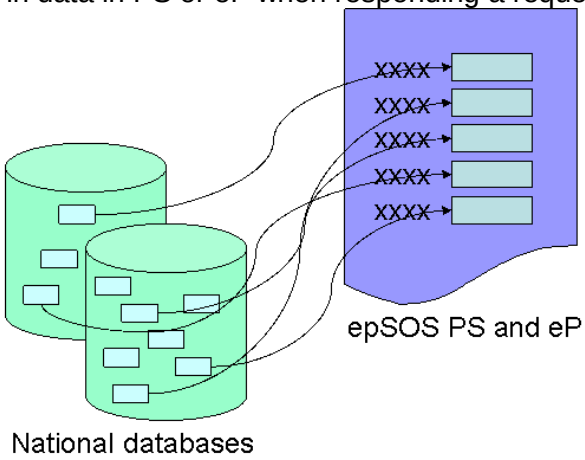


Figure 15: fields in the national databases mapped to fields in eHealth DSI PS, eP and eD

This mapping will be teamwork between technical experts knowing the structure of sources (e.g. database; document) from which the data are to be drawn and experts in coding on national level.

The Mapping allows to associate the sections/subsections of the Country A PS/eP/eD with the corresponding sections/subsections in the Pivot Document, based on CDA – PCC schema.

6.4.2 Transcoding and Mapping

The MTC will be used for translating the eHealth DSI codes from English (pivot format) to the language in country B. Non-codified data (like name and address) will not be translated. All countries in eHealth DSI must translate codes in MVC to the language in their own country, unless the eHealth DSI (English) designations are deemed to be understood and safely used by their Healthcare Professionals. The translation is included in the MTC of every specific Country. eHealth DSI countries which are only acting as country A may not need to do a complete translation, because they do not receive data from foreign countries. The translation in MTC is used for displaying the concepts in country B.

There is no easy way to deal with the translation and it must be solid and correct. Therefore, it needs to be done by experts and reviewed by clinicians. The mapping tool can be used for managing the translation processes. However, in some cases, for the International standard coding system (e.g. ATC, ICD10) official translations in several languages are already available. In these cases, the official translation will be preloaded in the eCRTS.

Below is a French/Swedish example of the transcoding/translation process:

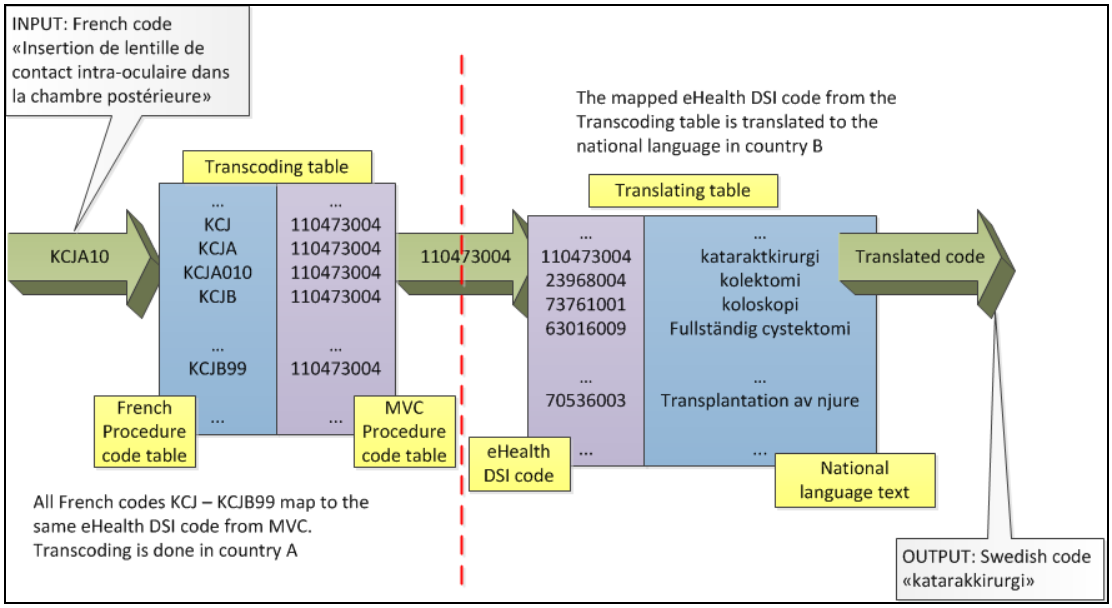


Figure 16: French/Swedish example of the transcoding/translation process

6.4.3 Semantic safety issues

It is an agreement that the semantic transformation of the medicine is based on the active ingredients and not on brand name[3].
When brand name substitution is of a product with a narrow therapeutic index and/or release, characteristics may be altered by a switch and patient safety considerations must be taken into account as alteration may result in either toxicity or under treatment.

Differences in package size; the countries must be able to recognise or translate the original medicine independently of the Package size so it can be changed.
If active ingredient, strength or pharmaceutical dose form of the medicine, as prescribed in country A, does not exist in country B, the medicine cannot be dispensed. Medicine can only be dispensed according to constitution of Country B.
As a safeguard, the original prescription should be received by pharmacist in country B[4]. Coding of information with currently available classification systems is strongly suggested to support semantic interoperability foreseen within the scope of the eHealth DSI.

6.4.4 MTC Maintenance

The activities related to MVC and MTC maintenance are described in [Semantic Services Specification]. Additional material can also be found in [Central Reference Terminology Server].
Some of the maintenance activities are triggered centrally, under the control of the eHealth DSI Terminology Responsible.
Example of such category is:

- Align MVC to new version releases of the official code systems.

Activities centrally triggered, but managed by deploying country are:

- Align the eHealth DSI MTC to the modified eHealth DSI MVC.

Other activities are triggered by the deploying country, but managed centrally, such as:

- Add to the eHealth DSI MVC the terms considered relevant by the deploying country and the experts concerning the eHealth DSI operation.

Finally some activities are triggered and managed by the deploying country, such

[3] [eP Functional requirements]
[4] [eP Functional requirements]

as:

- Update the eHealth DSI MTC with the necessary standard national changes.

The centrally managed maintenance activities require the supervision of the semantic expert team and the formal approval of the eHealth DSI Terminology Responsible.
The activities managed by the deploying country have to be validated by the deploying country terminology Responsible, with the supervision of the eHealth DSI Terminology Responsible.

It is highly advisable to exploit eCRTS to assure congruence and traceability of introduced changes.

7 Glossary

See [eHealth DSI Glossary].

8 References

[MLA] Multilateral Legal Agreement

Appendix A – Deployment Plan

In order to support a deploying country to plan Preparation and Deployment activities, a template with the most common activities (e.g. practices learnt from eHealth DSI Participating Nations) has been consolidated.

- eHDSI Service Deployment Plan (SDP) & Preparation Progress Report (PPR)

This template can also be used for sake of monitoring progress in a common way.

The template may evolve along the experience and practices gathered along the deployment activities.

Template available in eHealth DSI Specifications page