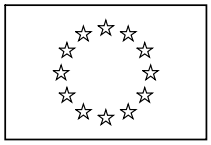

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
INFORMATICS
Information systems Directorate

European Commission

SML/SMP/eDelivery PKI Impact Assessment for the CEF eHealth DSI

Date:	06/01/2015
Version:	1.1
Author:	Adrien FERIAL
Contributors:	Dusko KARAKLAJIC Márcio SAMPAIO
Revised by:	Joao RODRIGUES FRADE
Approved by:	Joao RODRIGUES FRADE

Document History

Version	Date	Comment
0.1	14/10/2015	Initial draft version
1.0	16/12/2015	Testa-NG impact assessment Adaptation of the eDelivery PKI to a 3-tier certificate architecture Remarks from Markus KALLIOLA, Michèle FOUCART, SANDRO D'ORAZIO, Joao RODRIGUES FRADE and Masi MASSIMILIANO
1.1	23/12/2015	Modifications according to the remarks of Markus KALLIOLA: • Added executive summary • Added timeline for the PKI services

Contents

Acronyms

ABB	Architecture Building Block
ATNA	Audit Trail and Node Authentication
BDXL	Business Document Metadata Service Location
CA	Certificate Authority
CEF	Connecting Europe Facility
CRL	Certificate Revocation List
DSI	Digital Service Infrastructure
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
eCRTS	epSOS Central Reference Terminology Server
eIDAS	Electronic Identification and Signature
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IHE	Integrating the Health Care Enterprise – Europe
IPSEC	Internet Protocol Security
LSP	Large Scale Pilot
MoU	Memorandum of Understanding
MS	Member States
NCP	National Contact Point
NCP-A	National Contact Point of Country A
NCP-B	National Contact Point of Country B
NI	National Infrastructure
OCSP	Online Certificate Status Protocol
PEPPOL	Pan-European Public Procurement Online
PHI	Private Healthcare Information
PKI	Public Key Infrastructure
PN	Participant Nation

PoC	Point of Care
RA	Registration Authority
REST	Representational State Transfer
SHA	Secure Hash Algorithm
SML	Service Metadata Location
SMP	Service Metadata Publishing
TESTA	Trans European Services for Telematics between Administrations
TLS	Transport Layer Security
TSL	Trusted Service List
TTL	Time To Live
TSP	Trust Service Provider
VPN	Virtual Private Network

Glossary

DNSSEC: The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.

DSI: A Digital Service Infrastructure (DSI) enables networked services to be delivered electronically, typically over the internet, providing cross-border interoperable services for citizens, businesses and/or public authorities.

eDelivery: CEF Building block that enables secure and reliable exchange of structured, non-structured and/or binary data. Thematic DSIs such as eJustice, eProcurement, Social Security, etc. build their services by defining the content exchanged on top of eDelivery.[1]

e-SENS: e-SENS (Electronic Simple European Networked Services) is a large-scale pilot project with the aim of consolidating, improving, and extending technical solutions based around the building block DSIs to foster digital interaction with public administrations across the EU.

NCP: An epSOS NCP is an organisation legally mandated by the appropriate authority of each PN 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 organizations in order to provide the necessary services, which are needed to fulfil the epSOS Use Cases. The epSOS NCP is identifiable in both the epSOS domain and in its national domain. It acts as a communication gateway and also as a mediator for L&R aspects of delivering epSOS Services. As such, an NCP is an active part of the epSOS environment if it is compliant to normative epSOS interfaces in terms of structure, behaviour and security policy compliance.[2]

OpenNCP: epSOS NCP software publicly available under Open Source licensing

PKI: A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

SML: A Service Metadata Locator compliant with the e-SENS profile of the OASIS Business Document Metadata Service Location (BDXL) specification. The SML is used to add / update / delete information about the participants' SMP location on a Domain Name System (DNS). The SML is centralised.

SMP: A Service Metadata Publisher compliant with the e-SENS profile of the OASIS Service Metadata Publishing (SMP) specification. The SMP is a register of the message exchange capabilities and location of participants. The SMP is usually distributed.

TESTA: (Trans European Services for Telematics between Administrations) is a communication platform to exchange electronic data between European and Member States administrations in a secure, reliable and efficient way.

[1] eDelivery intro document

[2] http://www.epsos.eu/legal-background/the-national-contact-point-and-framework-agreement.html

Executive summary

1. Purpose

The purpose of this study is to:

- **Assess the impact of migrating the "Configuration Server" of epSOS to the "SML/SMP" architecture of the eDelivery DSI**. The Configuration Server is a central component in the epSOS project that provides the required configuration information to the countries for connecting each other. As part of the CEF eDelivery building block, the SMP and SML components provide a solution for dynamic service location and capability lookup.
- **Assess the impact of migrating the trust model of epSOS to the eDelivery dedicated PKI**. The trust model of epSOS is based on the fact that the National Contact Points (NCP) and their services are listed in the national trusted services lists. This is the key difference with the PKI based trust where it is assumed that NCP certificates are issued under the same root Certification Authority, which serves as a trust anchor for the participants in the network.
- Upon a request from DG SANTE, **assess the impacts of the replacement of the VPN network with TESTA services** from a technical viewpoint. A VPN is a technology that creates an encrypted connection over a less secure network. The TESTA network service provides a European backbone network for data exchange between a wide variety of public administrations. Both VPN and TESTA operates at the network layer and provides encryption capability.

2. Context

epSOS specifications were not fully implemented in the Large Scale Pilot (LSP) and some of the requirements were relaxed to ease the development. In particular, some security relaxations have been identified in the Configuration Server which is designed as an ad-hoc solution. The mission of EXPAND is to "bridge" eHealth assets to CEF. In this context, the Memorandum of Understanding (MoU) on operational activities for the CEF eHealth DSI between DG CONNECT, DG SANTE and DG DIGIT was created. This study was carried out by DIGIT as an activity of this MoU, for which one of the objectives is to assess the reusability of the CEF eDelivery building block within the CEF eHealth DSI. The main expected benefits are the removal of the security relaxations and an improved sustainability.

3. Methodology

To identify and evaluate the impact of migrating to the SMP/SML architecture, to TESTA or to the PKI model in use in eDelivery, the following approach was used: identify key stakeholders, collect and review the requirements, identify the relaxations of the pilots, propose the target architecture, perform a gap analysis to validate the target architecture, suggest a timeline for the migration and a roadmap.

To support the proposed approach, this study used interviews and meetings as a research method with the objective to voice the opinion of stakeholders and collect data and insight about the current implementation of the Configuration Server, the re-use of the SMP/SML architecture and TESTA-ng and the issues to tackle.

4. Results

SMP/SML: This study concludes that the SMP/SML is a standard and robust solution that seems to offer benefits to the eHealth domain and allows removing some relaxations introduced in the epSOS LSP. 10 change requests have been identified. Some of them are out of scope of the SMP specification and will be implemented by DIGIT. Other change requests require modification in the SMP specification and will be submitted by DIGIT to the stakeholder responsible for the maintenance of the specification in order to make the SMP more generic and more adapted to other domains.

This study provides a migration plan with the intent of moving progressively from the Configuration services to the SMP/SML architecture. The migration plan illustrates the activities that need to be conducted in order to reach the situation where all Participating Nations can start using the centralised SMP and SML components. According to the migration plan, this would start in August 2016 using an acceptance environment hosted by DIGIT. The estimation of the effort of DIGIT to support this migration is provided in this study.

PKI: From a technical perspective, moving to the dedicated PKI-based trust model of eDelivery offers some advantages: limited costs, ease of update and common configuration of the PKI services among the NCPs. However, legal factors may restrict the use of the dedicated PKI-based trust model of eDelivery. DIGIT and the PKI service provider are currently discussing the contract details. DIGIT expects the contract to be signed in February 2016 and the certificates to be available in March 2016.

TESTA: Assuming that the NCPs have access to TESTA, removing the VPN and using TESTA-ng instead is a move towards simplification that doesn't compromise security. However, it is important to note that these results need to be confirmed by the SNET team.

I. Introduction

This report is the deliverable of Activity 2 "SML/ SMP/eDelivery PKI Impact assessment" carried out by DIGIT in the context of the Memorandum of Understanding (MoU)[3] on operational activities for the CEF eHealth DSI between DG CONNECT, DG SANTE and DG DIGIT. The objectives of this document are twofold:

- Assess the impact of migrating the "Configuration Server" of epSOS to the "SML/SMP" architecture of the eDelivery DSI.
- Assess the impact of migrating the trust model of epSOS to a PKI-based trust model such as the one in use in the eProcurement domain by OpenPEPPOL.

Upon a request of DG SANTE, we also include in chapter "*II Target solution*" a section in which we assess the impacts of the replacement of the VPN network with TESTA-ng services from a technical viewpoint.

5. Scope

The configuration server in epSOS architecture is part of the "Shared services", formerly known as "virtual central services", which have a distribution point per NCP. The terminologies servers (eCRTS) are out of the scope of this document. The following figure therefore illustrates the scope of the services to be replaced by SMP/SML:

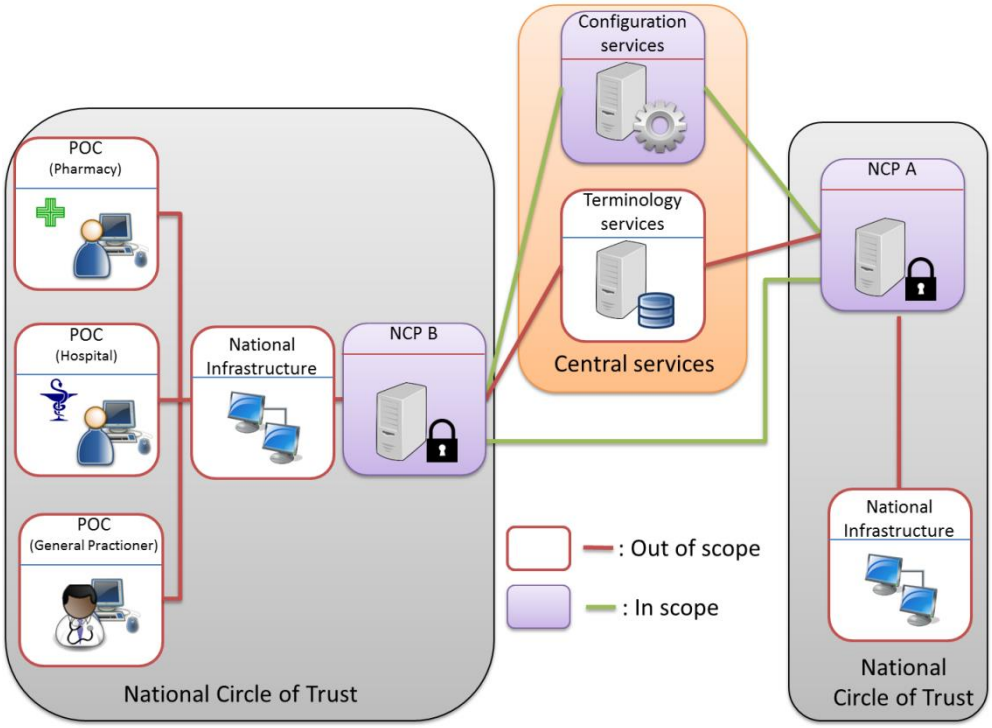

Figure 1 - epSOS network overview, baseline architecture

[3] Memorandum of Understanding (MoU) on operational activities for the CEF eHealth DSI between the DG CONNECT, DG SANTE and DG DIGIT, 29/07/2015

It is important to note that SMP and SML were initiated by PEPPOL[4]. At the end of August 2012, the PEPPOL project was finalised and its services and responsibilities were taken over by the non-profit association OpenPEPPOL.

The PEPPOL SMP and SML specifications were submitted as inputs to the OASIS BDXR TC (Business Document Exchange Technical Committee) with the intent of defining a standardized and federated document transport infrastructure for business document exchange. They resulted into 2 new committee specifications: SMP (Service Metadata Publishing)[5] and BDXL (Business Document Metadata Service Location)[6].

The table below summarises it:

Original input specification	OASIS committee specification
PEPPOL Transport Infrastructure Service Metadata Locator (SML)[7]	Business Document Metadata Service Location (BDXL)
PEPPOL Transport Infrastructure Service Metadata Publishing (SMP)[8]	Service Metadata Publishing (SMP)

Table 1 – PEPPOL to OASIS specifications

In WP6[9], e-SENS defines 6 ABBs (Architecture Building Blocks) for eDelivery: Transport of Data, Capability Lookup, Addressing of Entities, Service Location, Backend Integration and End to End Evidences. Only Service Location ABB and Capability Lookup ABB are in-scope for this document. Other ABBs are out of scope. e-SENS provides implementation guidelines for these 2 ABBs based upon OASIS SMP and BDXL specifications, and maintain compliance with the legacy SML specification.

In this document, we use the following terminology:

- SMP refers to the OASIS version of the specification.
- SML references the Solution Building Block (SBB) that implements the Service Location ABB of e-SENS, and is compliant with the legacy SML from PEPPOL and with OASIS BDXL.

The main focus of this document is on the reuse of the building blocks from a technical perspective. All other types of barriers that may hinder or delay the reuse of the building blocks are outside of scope (mainly legal and organisational factors).

The scope of this assessment is to evaluate the impact of the replacement of the Configuration Server and of the epSOS trust model. The impacts are evaluated on both eDelivery and OpenNCP components.

[4] PEPPOL (Pan-European Public Procurement Online), http://www.peppol.eu/
[5] OASIS Service Metadata Publishing (SMP) Version 1.0, http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html
[6] OASIS, Business Document Metadata Service Location Version 1.0, http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html
[7] PEPPOL Transport Infrastructure Service Metadata Locator (SML), Version 1.0.1, https://joinup.ec.europa.eu/svn/peppol/PEPPOL_EIA/1-ICT_Architecture/1-ICT-Transport_Infrastructure/13-ICT-Models/ICT-Transport-SML_Service_Specification-101.pdf
[8] PEPPOL Transport Infrastructure Service Metadata Publishing (SMP), Version: 1.1.0 https://joinup.ec.europa.eu/svn/peppol/PEPPOL_EIA/1-ICT_Architecture/1-ICT-Transport_Infrastructure/13-ICT-Models/ICT-Transport-SMP_Service_Specification-110.pdf
[9] Work Package 6, eSens, http://wiki.ds.unipi.gr/display/ESENS/e-SENS+WP6+Project

6. Background

The epSOS project was co-funded by the European Commission Competitiveness and Innovation Programme (CIP) within the ICT Policy Support Programme. epSOS aimed to design, build and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe. The project period started in 2008 and ended in 2014.

EXPAND (Expanding Health Data Interoperability Services)[10] is a Thematic Network whose main goal is to progress towards an environment of sustainable cross border eHealth services, established at EU level by the Connecting Europe Facility (CEF) and at national level, through the deployment of suitable national infrastructures and services. EXPAND maintains, updates and upraises epSOS assets and prepares them for their hand over to CEF. The duration of the project is 24 months, from 1st January 2014 to 31st December 2015.

CEF is currently promoting the deployment of 5 highly reusable building blocks, enablers of interoperability across borders and also across policy domains. These are: eDelivery, eID, eSignature, Machine Translation and eInvoicing. Except for Machine Translation, they have been developed in the Large Scale Pilots and are currently being consolidated through the e-SENS (the last Large Scale Pilot). CEF is mandated to deploy and evolve these building blocks as well as potentially include new ones that have been developed in other settings such as e-SENS, ISA or H2020. The building blocks of CEF are solutions and services that will form part of a wide variety of IT systems, in different policy areas, supporting the delivery of digital public services across borders.

epSOS specifications were not fully implemented in the LSP (Large Scale Pilot) and some of the requirements were relaxed to ease the development. In order to remove some (or all) of the relaxations, e-SENS (Electronic Simple European Networked Services) is pushing into the eHealth domain a building block based on the SMP/SML architecture. The overall purpose of implementing e-SENS building blocks in the e-Health domain is to improve efficiency, cost-effectiveness, safety and confidence in cross-border health care.

Some security relaxations related to the Central Services have been identified in the "WP5.2 eHealth cross border central services status quo and outlook"[11] document from e-SENS. These security relaxations are not suitable in an operational environment as they break compliance with the IHE specifications, reduce interoperability and lead to security risks:

ID	Relaxation	Comment
1	Certificates in use in the pilots don't comply with the recommended certificate profiles defined in D3.A.7 – epSOS EED X.509 Certificate Profiles	e-SENS concluded that replacing the Configuration Server with the SMP/SML architecture "*doesn't restrict the provision of epSOS compliant certificates by member states, it's up to them to fulfil this requirement.*"[11] According to DIGIT, the use of the dedicated PKI-based trust model can help to remove this relaxation because it introduces a common configuration among the NCPs.

[10] EXPAND, http://www.expandproject.eu/

[11] WP5.2 eHealth cross border central services status quo and outlook, version 0.3, 2015

2	Lack of VPN connection between central services and NCPs	e-SENS concluded that replacing the Configuration Server with the SMP/SML architecture "*removes the need for a VPN connection between central services and NCPs*"[11]
3	OpenNCPs are not ATNA Secure Nodes	Replacing the Configuration Server with the SMP/SML architecture helps to eliminate this relaxation because it removes the need for TSL-Sync and SyncApp. e-SENS concluded that "*the ATNA log files format is still an issue, which was not intended to be solved by SMP/SML (out of scope).*"[11]
4	epSOS trust bootstrap was relaxed by using the mutually-acknowledged TSL file	e-SENS concluded that SMP/SML "*does not create any major constraint on the usage of certificates.*"[11] According to DIGIT , the use of the dedicated PKI-based trust model can help to remove this relaxation because the certificates are issued under the same root CA

Table 2 - Security relaxations

Other issues have also been identified:

- Configuration services are designed as an ad-hoc solution for the needs of eHealth
- Knowledge was lost regarding the current implementation because of a change in the central services provider and a lack of documentation. e-SENS experts had to reverse engineer the SyncApp script to get a better understanding[11] of its features
- The implemented version doesn't fully comply with the specification and has some security relaxations regarding the certificates (security relaxation ID4)

For all the above reasons, it was decided to evaluate the replacement of the Configuration Services with the candidate SMP/SML architecture. According to DIGIT, such architecture offers the following benefits:

ID	SMP/SML benefits	Implication for eHealth
1	Standard from OASIS	Helps to ensure safety, reliability, robustness and enhance interoperability
2	Ability to manage an increasing number of participants to the message exchange network	Facilitates the registration of new NCPs in the eHealth network
3	Ensure that the addresses of participants can be easily changed and discovered	Removes a single point of failure if the SMPs are distributed
4	Make information about the participants (what messages they can process, the message protocol that they support, …) available to everyone in the data exchange network	Avoid the need for manual configuration and removes the need for using scripts like TSL-Sync and SyncApp

Table 3 - SMP/SML benefits

The replacement of the epSOS trust model by a dedicated PKI-based trust model is also considered in this report. According to DIGIT, the following benefits are expected:

- Removal of security relaxations 1 & 4
- Limited costs
- Easy-to-update
- Common configuration of the PKI services among the NCPs

7. Impact assessment methodology

To identify and evaluate the impact of migrating to the SMP/SML architecture and to the PKI model in use in eDelivery, the following approach is used:

- Identify key stakeholders
- Collect and review the requirements, identify the relaxations of the pilots
- Propose the target architecture
- Perform a gap analysis to validate the target architecture
- Suggest a timeline for the migration and a roadmap

To support the proposed approach, this study used interviews and meetings as a research method with the objective to voice the opinion of stakeholders and collect data and insight about the current implementation of the Configuration Services, the re-use of the SMP/SML architecture and the issues to tackle.

A continuous dialogue was kept with representatives from DG SANTE, e-SENS and the OpenNCP community.

Date	Interviewee/Event	Notes
	Participation to meetings with the OpenNCP about the integration with SMP	Meeting minutes of 09/09/2015[12] Meeting minutes of 11/09/2015[13] Meeting minutes of 18/09/2015[14]
17/09/2015	Interview of Masi MASSIMILIANO (e-SENS)	See meeting minutes in ANNEX 1
22/09/2015	Interview of Uwe ROTH (e-SENS) and João GONCALES (e-SENS)	
24/09/2015	Interview of Yacoubou WAOLANY (SANTE)	See meeting minutes in ANNEX 2
22/09/2015	Interview with SANTE	See meeting minutes in ANNEX 3
15/10/2015	Meeting with DG SANTE and e-SENS	See meeting minutes of 15/10/2015[15]
17/11/2015	Interview with Otman DAHEL (DIGIT/ TESTA)	
03/11/2015	Review of comments from DG SANTE	

Table 4 - Interview plan

[12] https://openncp.atlassian.net/wiki/display/ncp/20150909+-+Meeting+minutes%2C+Wednesday%2C+September+9th%2C+2015+-+OpenNCP+integration+with+SMP
[13] https://openncp.atlassian.net/wiki/display/ncp/20150911+-+Meeting+minutes%2C+Friday%2C+September+11th%2C+2015+-+OpenNCP+integration+with+SMP
[14] https://openncp.atlassian.net/wiki/display/ncp/20150918+-+Meeting+minutes%2C+Friday%2C+September+18th%2C+2015+-+OpenNCP+integration+with+SMP
[15] https://openncp.atlassian.net/wiki/display/ncp/20151015+-+Meeting+minutes%2C+Thursday%2C+October+15th%2C+2015+-+OpenNCP+integration+with+SMP

II. Target solution

It is important to note that the migrations to TESTA, to the eDelivery PKI or to the SMP/SML model are 3 independent topics. They have no coupling with each other and therefore it can be decided to implement one, two or the three migrations.

1. Replacing the configuration Server

The target solution is to replace the configuration server with a SMP/SML-based solution. Many discussions where held within the OpenNCP community to identify and tackle the issues raised by such a migration. In this chapter, we describe and provide an overview of the target solution, a description of the transition plan and we identify the impacts on the components.

a) Migration plan overview

To mitigate the risk of the migration, DIGIT recommends a transition plan with the intent to move progressively from a centralised SMP to distributed SMPs hosted by the Participating Nations (PNs). This transition plan is in line with the discussions held with the participants of the OpenNCP community regarding the migration to the SMP/SML architecture. Of course, this plan needs to be validated by DG SANTE and CEF:

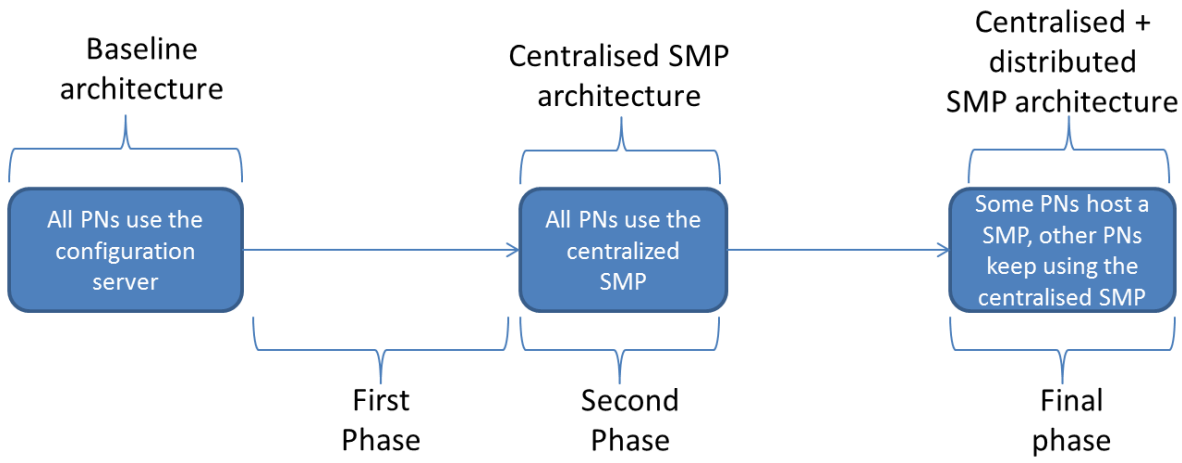

Figure 2 - Migration plan overview

- **First phase**: the current configuration server remains up and running while a centralised SMP is deployed. During this phase, only a set of selected and voluntary Participating Nations migrate their configuration to the centralised SMP. These Participating Nations are required to maintain their configuration simultaneously on the SMP and on the configuration server. This is to avoid regression for the other Participating Nations during this phase, as they will still use the configuration server. The first phase is finished when all the selected countries have moved their metadata to the centralised SMP and when the migration process is approved. This is the first transition architecture of the migration plan.

Component	Hosting
Configuration server	DIGIT
SMP	DIGIT
SML	DIGIT

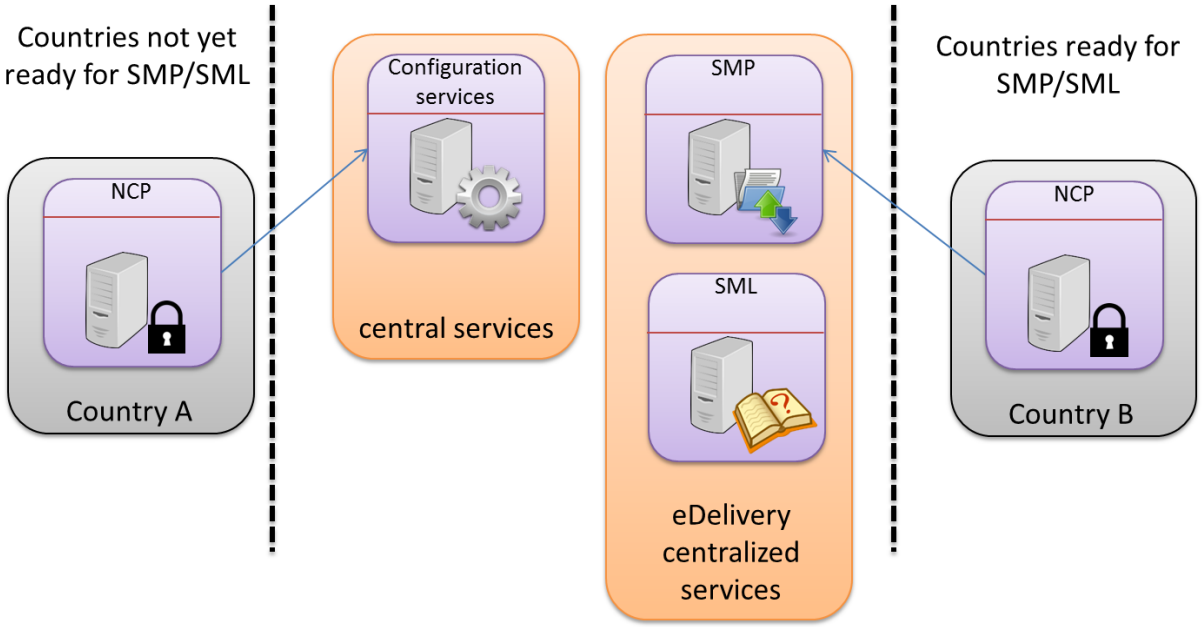

Figure 3 - First phase, first transition architecture

- **Second phase**: When the use of the centralised SMP is validated by the voluntary Participating Nations, all Participating Nations are required to use the centralised SMP and the configuration server is shutdown. This is the pilot architecture of the migration plan. A more detailed migration plan to reach this phase is described in chapter "*V Migration plan*".

Component	Hosting
SMP	DIGIT
SML	DIGIT

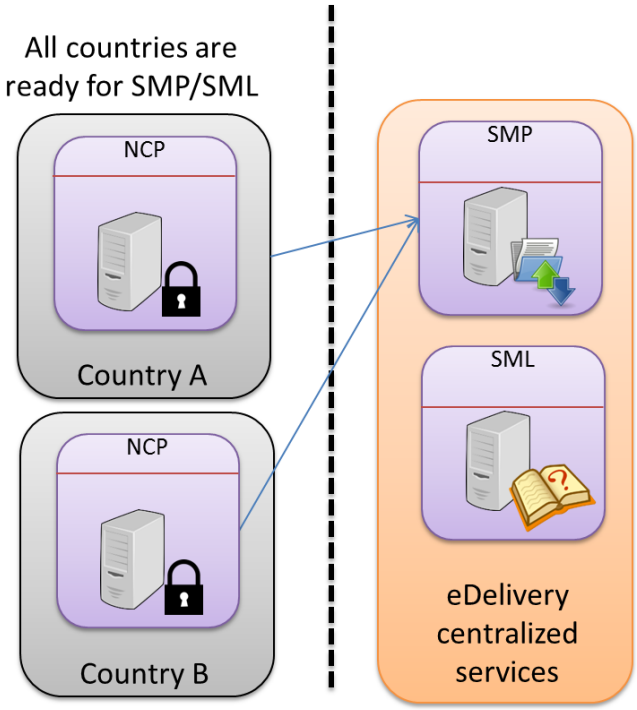

Figure 4 - Second phase: centralised SMP, second transition architecture

- **Final phase**: In this phase, the centralised SMP server remains up and running while selected Participating Nations start hosting their own SMP. Once a country hosts its SMP, the metadata for the corresponding NCP are removed from the centralised SMP and the DNS records are updated by the SML. The pre-final phase is finished when all the selected countries have moved their metadata and when the migration process is approved. This is the target architecture of the migration plan.

Component	Hosting
Centralised SMP	DIGIT
Distributed SMP	Countries host their own SMP
SML	DIGIT

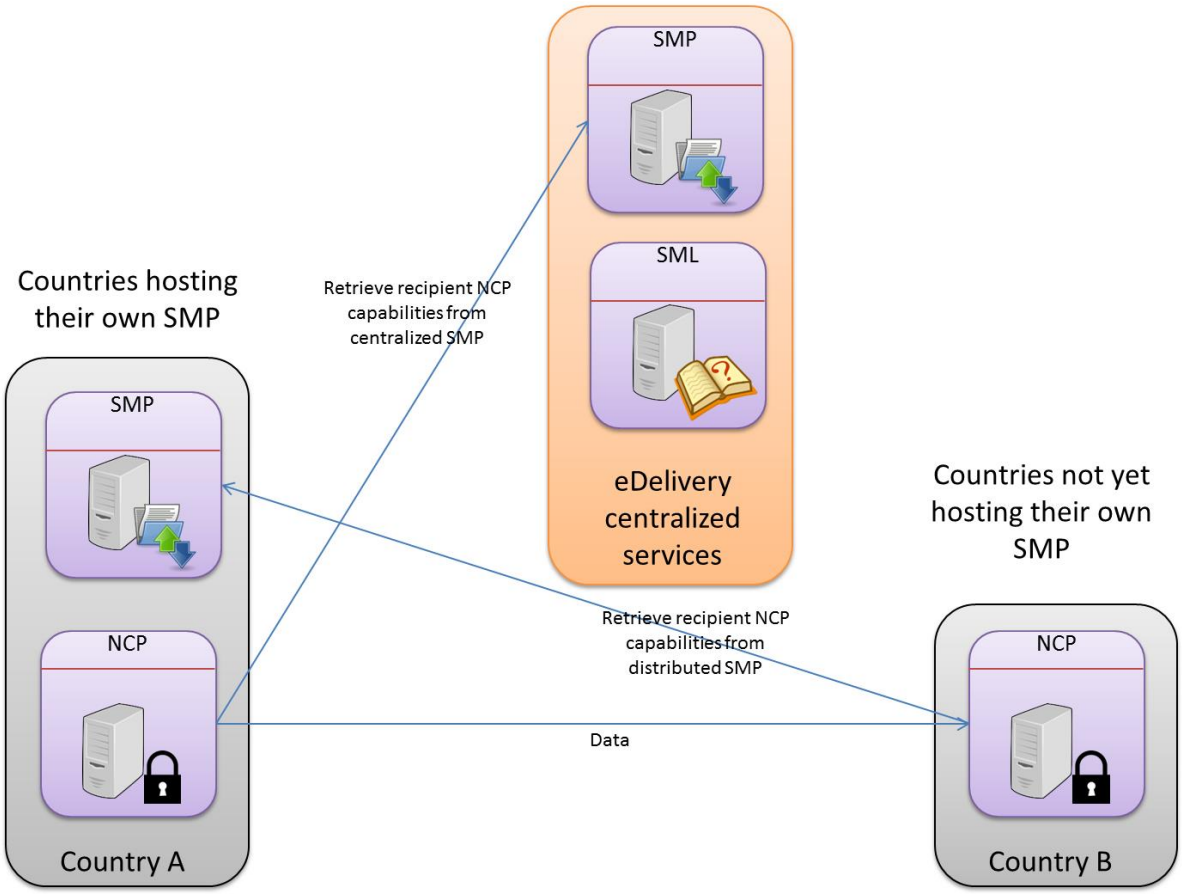

Figure 5 –Final phase: centralised SMP and distributed, target architecture

- **Suggested architecture (optional):** The recommendation of DIGIT is to encourage the PNs to host their own SMP. Indeed, the more the PNs host their SMP, the more the risk of a single point of failure diminishes. DIGIT recommends the central SMP to be used only by the PNs that don't have the capability to host their own SMP. In the event all PNs agree on hosting their own SMP, then the central SMP could be removed. This is the preferred solution according to DIGIT, but it remains only an option: it is the PNs responsibility to decide whether they host their own SMP or not.

Component	Hosting
SMP	Each country hosts its own SMP
SML	DIGIT

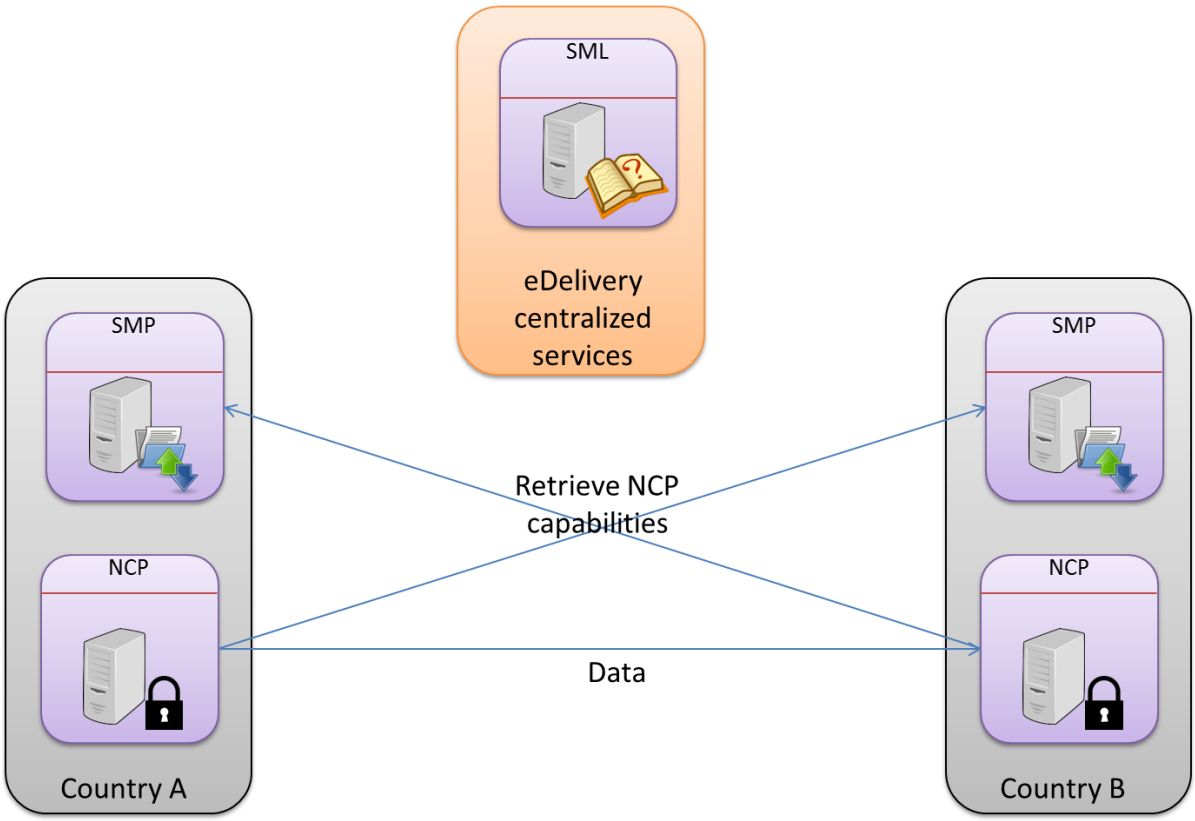

Figure 6 – Preferred architecture (optional only), distributed SMPs

b) Impacts on NCP of the migration to the target solution

In this section, we describe the impacts of the migration for the OpenNCP implementation. However, for practical reasons, we use the generic term NCP to refer to the OpenNCP implementation.

As a result of several meetings with DG SANTE, the following main impacts on the use cases of NCP have been identified. To ensure that no element is missing, DIGIT recommends DG SANTE to analyse the impacts in more detail:

Use case	Current implementation	Target solution
Publish metadata	Edit and upload TSL files to the configuration server with TSL-editor	Edit and upload metadata to the SMP with SMP-editor
Fetch metadata of the recipient NCP	Retrieve periodically the configuration from the configuration server with TSL-Sync script, and store it in the database.	Configuration is retrieved on-demand, just before executing the use case "Send data"
Send data	Retrieve the configuration from the local database and send the data	Look in the memory cache if the configuration from the recipient is known and valid. If so, then use this configuration to send the message. Otherwise, retrieve the configuration from the SMP and store it in the memory cache

i. Publish metadata use case

The TSL-editor software currently used to edit and upload the TSL files to the configuration will be replaced or converted into a SMP-editor that will call the REST services from the SMP. The process remains pretty identical from the viewpoint of the user.

Current implementation for the use case "Publish metadata":

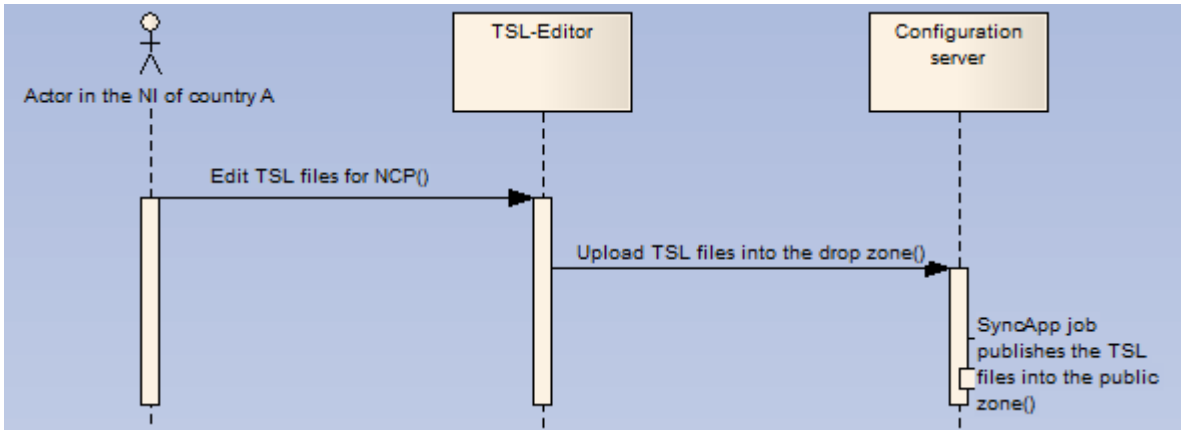

Figure 7 - Sequence diagram of the "Publish metadata" use case for the current implementation

Target solution for the use case "Publish metadata":

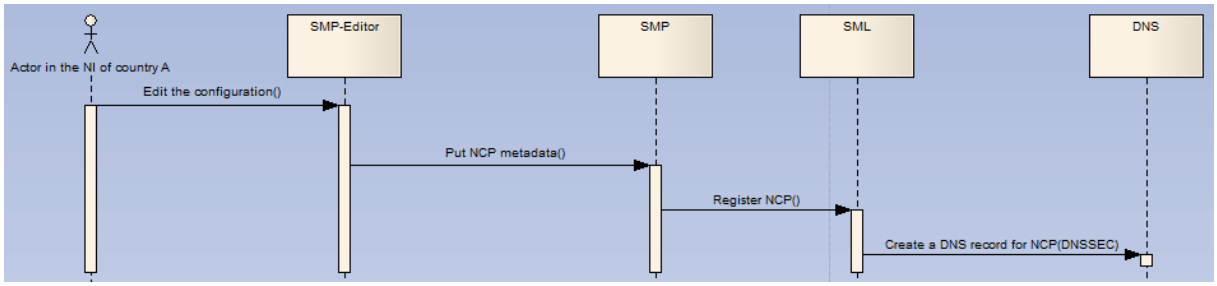

Figure 8 - Sequence diagram of the "Publish metadata" use case for the target solution

ii. Fetch metadata and send message use cases

The use case "Fetch metadata from other NCPs" is different in the current implementation and in the target solution. In the current solution, the configuration of the other NCPs is periodically fetched from the configuration server and stored in a local database. In the target solution, NCPs won't store any metadata in the database: instead, NCPs will use an in-memory cache with a pre-defined Time-To-Live (TTL). Once the cache is invalid, the metadata will be fetched again from the SMP.

The cache is invalid if the TTL expired, or if a particular type of exception (the hierarchy of countable exceptions still needs to be defined) is raised while trying to contact an endpoint using the cached metadata.

Current implementation for the use case "Fetch metadata" and "Send message":

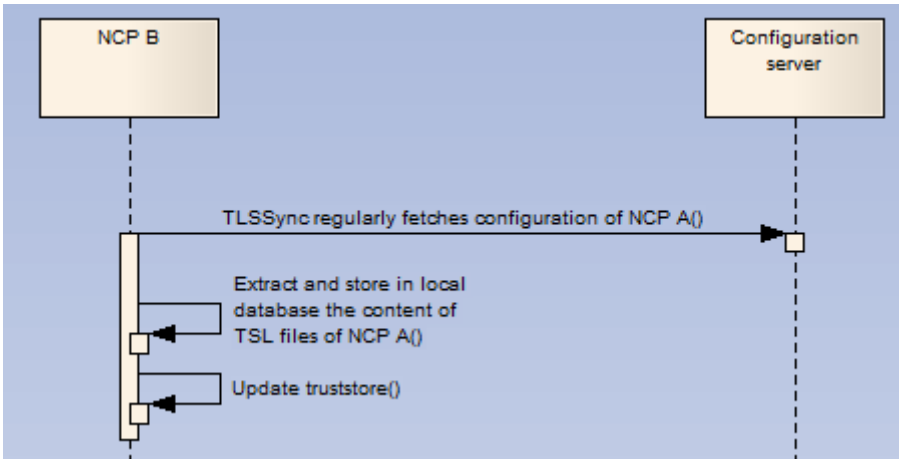

Figure 9 - Sequence diagram of the "Fetch metadata" use case for the current implementation

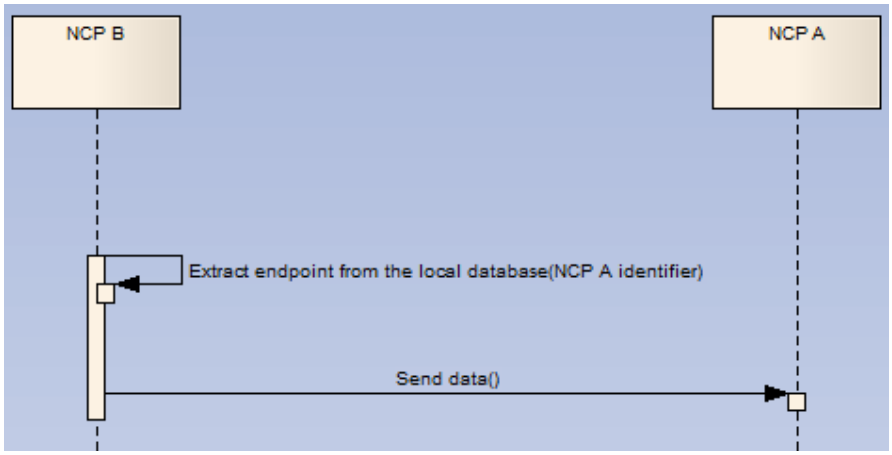

Figure 10 - Sequence diagram of the "Send message" use case for the current implementation

Target solution for the use case "Fetch metadata" and "Send message":

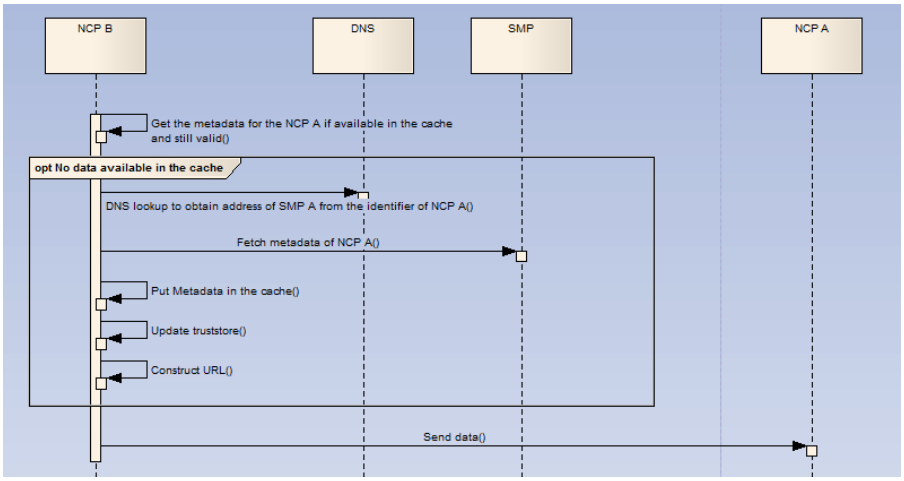

Figure 11 - Sequence diagram of the "Fetch metadata" and the "Send message" use cases for the target solution

iii. Impact on the logical components of the NCP

An analysis performed by SANTE[16] showed that the construction of the URLs is always performed like below:

String epr = ConfigurationManagerService.getInstance().getServiceWSE(countryCode.toLowerCase(Locale.ENGLISH), service);

The Configuration Manager is the central component for the construction of the URL and the resolution of the endpoints. It is included in the ClientConnector and this latter component will be impacted with the migration to the SMP/SML architecture.

To retrieve the metadata, a SMP client library (provided by DIGIT) needs to be integrated with the NCP. This SMP client helps to define the endpoint for a given resource, and hides the complexity of this process. The SMP client can also be integrated into the ClientConnector logical component, together with the caching layer.

It is not excluded that other components may be impacted by the migration. Indeed, it is not yet clear whether some refactoring in the current OpenNCP implementation to make it fully compliant with the reference documentation is required. This topic still needs to be discussed within the OpenNCP community. However, changes are considered to be limited and isolated.

c) Impacts on the SML

DIGIT must provide SML services compliant with the Service Location ABB[17] requirements. No specific impact on the current SML and BDXL specification were identified. However, DIGIT needs to perform some advanced testing to confirm that its reference implementation can support multiple domains. Especially, some domains require the use of DNSSEC (like eHealth) while others don't and both configuration should be supported on the same running environment.

Note that on December 2015, DIGIT doesn't yet provide DNSSEC services (see section *IV.3 Open issues and questions* for further details)

d) Impacts on the SMP

Some impacts have been identified regarding the SMP specification. Some of them are listed in the "epSOS Change Proposal" from Masi Massimiliano[18]. This document was written in the context of EXPAND with the objective to update the epSOS specification for the SMP/SML architecture. Some other impacts on the SMP were also discussed during meetings. As a result, DIGIT will group them and prepare a set of change requests and submit them to e-SENS.

6 change requests are non-blocking and are optional for the live implementation.

3 change requests are required for the live implementation and are already tackled either by DIGIT or by an agreement of the OASIS TC on an update of the specification. Thus they are considered as non-blocking.

1 change request is blocking and has been identified as an open issue that needs to be discussed together with e-SENS and DG SANTE.

[16] See ANNEX 4
[17] ABB - Service Location: http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Service+Location
[18] epSOS Change Proposal v0.4: CP-epSOS-SMP-v0.4.docx

All the necessary information about these change requests is listed in chapter "*2 Change requests*".

e) Timeline

This is a linear representation of the major milestones and a rough estimate of the duration of the different phases. DG SANTE is responsible for the onboarding of the PNs while DIGIT is responsible for delivering SMP/SML services and support.

The EXPANDATHON event happening from 9th to 11th December 2015 will help to validate the feasibility of the replacement of the Configuration Server with SMP/SML. The event aims are:

- To convey the results of EXPAND, creating critical mass among the different Stakeholders in preparation of deployment of CEF cross-border eHealth services.
- To collect testimonials about how the results of the EXPAND have been contributing to the readiness of Stakeholders concerning cross-border eHealth services deployment.
- To give Member States the opportunity to assess their readiness for deployment of cross-border eHealth services.
- Disseminate to and engagement of a wider arena, including patients and health professionals.

During this event, the integration between an adapted version of the OpenNCP implementation and the current SMP implementation will be tested. The results and the lessons learned will allow DG SANTE and the OpenNCP community to start the adaptation of the OpenNCP.

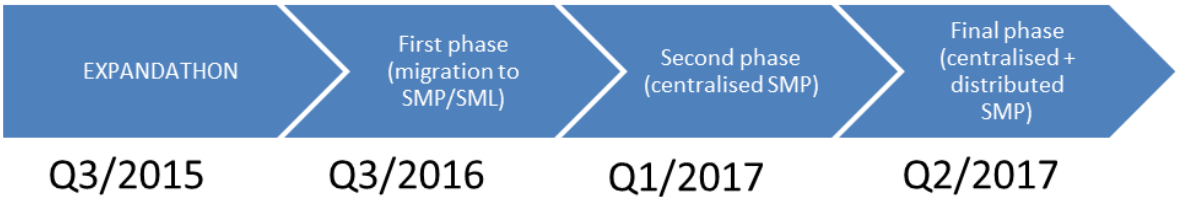

Figure 12 - Timeline

f) Cost distribution

DG SANTE will contribute to the costs of the dedicated centralised SMP and SML services and the related support. According to DIGIT, a rough estimate of the costs would be, for 3-year service availability:

- Setting up the centralised services and support for the first year: estimated at 100k€
- Running the centralised services and support for a period of 2 years: estimated at 100 k€

The *Activity 5 Hosting of the central services (configuration server and terminology services)* of the MoU already includes the hosting of the SMP and SML components.

In the next MoU, DG SANTE will order a study to be carried out by the unit DIGIT C regarding the provision of DNSSEC services. DG SANTE will entirely finance the costs of this study.

2. Replacing the trust model of epSOS

In the current trust model of epSOS, the nation's trust anchor is the National Trust Service Provider (TSP). Directive 1999/93/EC[19] stipulates that there is direct trust between TSPs from different nations. The TSL trust model is based on the fact that the NCPs and their services are listed in the national trusted services lists (TSL). This is the key difference with the PKI based trust where it is assumed that NCP certificates are issued under the same root CA, which serves as a trust anchor for the participants in the network.

The assessment of the replacement of the trust model of epSOS by a dedicated PKI-based trust model is an initiative from DG SANTE. There is no prior work on this subject performed by e-SENS.

From a technical perspective, the main consequences of the replacement of the trust model of epSOS are the configuration of the list of trusted certificates and a change in the validation process of the trust. With the current trust model of epSOS, it is required to verify if the originating TSP is listed on the corresponding national TSL while in the dedicated PKI-based trust model, a certification path is built, e.g. the list of all intermediate CAs up to the root one.

As explained in section *III.3 Security*, the eDelivery PKI uses a 3-Tier Certificate architecture and a "closed user group". The sub-levels of the PKI are not delivered by sub-CAs but follow a convention represented in the certificate metadata. It means that the evaluation of the trust in the eDelivery components and in the NCP must be performed in a 2-phase process:

1. Check the trust anchor from the certification path
2. Programmatically analyse the "subject" and the "issuer" attributes to check if the certificate was delivered by the eHealth sub-RA

Technical impacts are limited but legal and organisational factors may restrict the use of the dedicated PKI-based trust model of eDelivery. These factors are not discussed in this document as they are out of scope.

a) Migration plan overview

The migration to the dedicated PKI-based trust model can take place into 5 steps:

- Each PN requests certificates from the adequate Registration Authority (RA)
- The Certificate Authorities (CA) issues the requested certificates
- The PNs install the certificates on their NCP
- The PNs update the trust configuration of their NI nodes with their NCP certificates
- DIGIT installs the certificates on the SML and the SMP

This migration can be performed independently of the migration to the SMP/SML architecture.

b) Impacts on the NCP

The migration to a dedicated PKI-based model would mainly affect the SecurityManager. The SecurityManager is used for certificate validation and XML-Signature creation and validation. With the current epSOS trust model, it maintains a list of all trusted certificates available in order to check

[19] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:31999L0093

whether the given certificate is a member of the Circle of Trust. The certificate validation includes a mathematical check, a validity check and the OCSP call[20]. As a consequence of the migration to the PKI model, the configuration of the trusted certificates will be changed and the SecurityManager will be modified to integrate the control of the attributes of the certificate metadata based on the "closed user group" conventions (see section *III.3 Security* for further details*)*.

There is also an impact identified on the National Infrastructure (NI) of each participating nation. Because the NCP certificates won't be issued under a national root CA, the NCP certificates would need to be added to the list of trusted certificates on each node of the NI.

c) Impacts on the SML

No impacts on the current SML and BDXL specification were identified. The SML implementation supported by DIGIT is not impacted.

d) Impacts on the SMP

No impacts on the current SMP specification were identified. The SMP implementation supported by DIGIT is not impacted.

e) Cost distribution

Most of the PKI expenses are covered by DG CONNECT. eHealth will be responsible for running the RA service.

f) Timeline

The "Specific contract for PKI services" and the "Service Work Order" are now drafted and will be discussed in January 2016. DIGIT expects the contract to be signed in February 2016 and the first certificates to be available in March 2016.

On 14th January 2016, a PKI workshop will be organised by the PKI service provider Telesec. This workshop will be the opportunity for DIGIT to learn more about the processes to set up in order to provide support for PKI services.

3. Replacing the VPN between NCPs with TESTA-ng

Important note: This chapter introduces the results of the study carried out by DIGIT regarding the replacement of the VPN by TESTA-ng. They are presented as they are understood by DIGIT after multiple meetings handled with DG SANTE and the TESTA team. The SNET team still needs to confirm the feasibility of this study (see section IV.3 Open issues and questions for further details).

The current epSOS specification mandates the use of a gateway-to-gateway virtual private network (VPN)[21]. A VPN is a technology that creates an encrypted connection over a less secure network. The benefit of using a VPN is that it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it[22]. The feedback from the epSOS pilot regarding the VPN shows that its configuration was difficult mainly

[20] http://www.epsos.eu/technical-background/reference-implementation/core-elements.html
[21] D3.4.2 epSOS Common Components Specification – section 4.1.1 IPSec Configuration
[22] http://searchenterprisewan.techtarget.com/definition/virtual-private-network

because of interoperability issues[23]. For this reason, it has been decided to evaluate the use of TESTA for the connection between the NCPs, in replacement of VPN over internet:

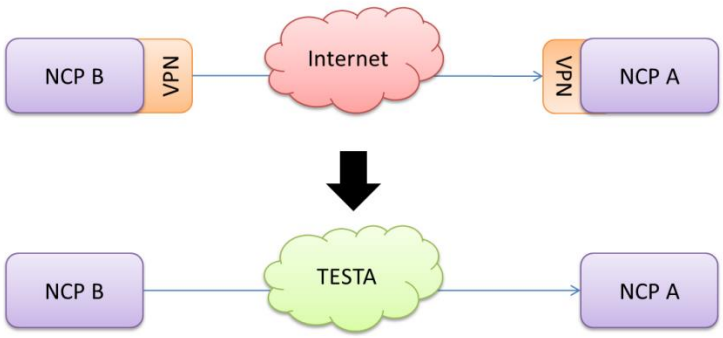

Figure 13 - Moving to TESTA-ng: Target solution

In this document, we don't discuss the availability of TESTA: we assume that all NCPs can connect to TESTA, either via their national network or via a TESTA gate. The study of the availability of TESTA is performed in the activity 3 of the MoU[3]: "*feasibility study on the implementation of the connections between the eHealth NCPs using the TESTA national networks*". It is the responsibility of the PN to connect to TESTA and obtain an address in "testa.eu" for their NCP.

The TESTA[24] network service provides a European backbone network for data exchange between a wide variety of public administrations. The network uses the Internet Protocols (IP) to ensure universal reach, but is operated by the EU Commission separately from the Internet. It provides guaranteed performance, high levels of security and has connections with all the EU Institutions and national networks. It caters for the exchange of both unclassified and classified information. TESTA was launched in 1996 and evolved a lot since, adding new valuable services at each generation. The newest 4th generation named TESTA-ng is planned for February 2016.

Both VPN and TESTA operates at the network layer and provides IPSEC (Internet Protocol Security) encryption. From a security standpoint, both solutions are equivalent and provide encryption at network layer.

The central components (SML, centralised SMP, DNS) are hosted at the European Commission datacentre, which is already connected to TESTA. For this reason, it is technically possible to map their internal addresses to external "testa.eu" and "europa.eu" addresses (to be confirmed by the SNET team, see section *IV.3 Open issues and questions* for further details). In this case, all the centralised and distributed components can be available on the "testa.eu" domain:

[23] https://openncp.atlassian.net/wiki/display/ODC/VPN+problems+tracking+and+resolution
[24] Strengthening the EU's telecommunications backbone: http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-4action_en.htm

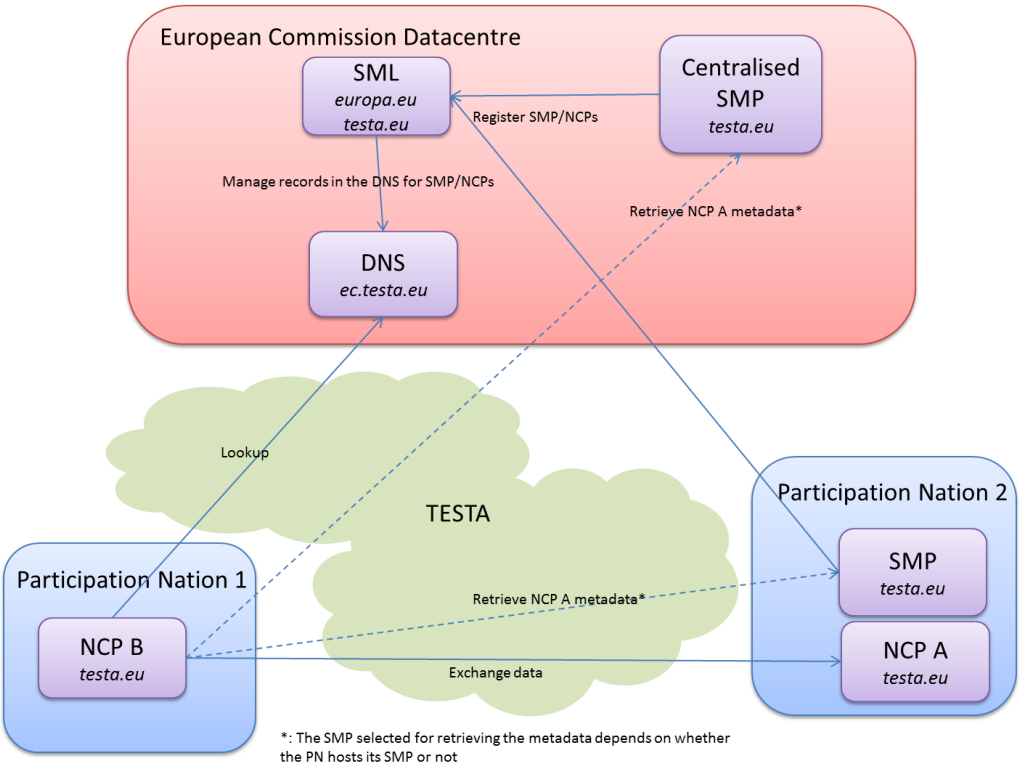

Figure 14 - DNS domains distribution

Note: the picture above only shows components in use in eHealth. In the actual deployment model, there are also an internal intermediary DNS server and another DNS server available on the Internet for the addresses in "ec.europa.eu" but it is not illustrated for simplification purposes. Components of other domains are also not represented.

a) Impacts on the NCP

The TSL files contain the entry "epSOS VPN Gateways status information" which announces the address and digital certificate of a NCP's VPN gateway. In order to establish the VPN connection, the NCP B must retrieve the VPN gateway information of NCP A and configure the VPN client:

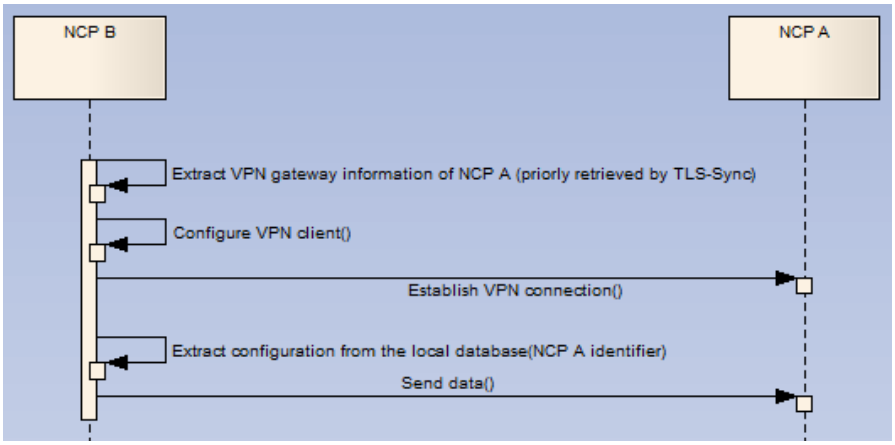

Figure 15 - Establishing the VPN connection

If TESTA network is used, there is no need for a VPN. NCP B still needs to extract information regarding the NCP A endpoint but doesn't need any VPN certificate. The sequence diagram would

then be much simpler as in *Figure 10 - Sequence diagram of the "Send message" use case for the current implementation*). Therefore, the entry "epSOS VPN Gateways status information" would be removed from the TSL files.

Both solutions require firewall configuration in order to enable the establishment of the connection. There is no automatic configuration in the current OpenNCP implementation, the setup of the firewall is manual and remains as such with TESTA. It is possible to script the configuration of the firewall rules but this topic is out of scope of this document.

As a conclusion, assuming that the NCPs have access to TESTA, the removal of the VPN is a move towards simplification and doesn't compromise security.

b) Impacts on the SML

The SML hosted at DIGIT puts the records into an intermediary DNS. Then an internal synchronisation process replicates the records to DNS servers available on the internet and on the TESTA network. Therefore, the TESTA DNS is available for the NCPs. As a consequence:

- No change is required on the SML and the DNS because they are already available in TESTA. Only the configuration changes: for the eHealth project, the DNS domain configured would be "edelivery.tech.ec.testa.eu" instead of "edelivery.tech.ec.europa.eu".
- Because the TESTA DNS is used, there is no need for DNSSEC. Indeed the level of security provided by the network layer prevents the risks of DNS spoofing.
- A request for an external mapping in the "testa.eu" domain must be submitted to SNET by DIGIT CIPA

c) Impacts on the SMP

No impact was identified for the SMP component.

For the centralised SMP a request for an external mapping in the "testa.eu" domain must be sent to SNET.

d) Cost distribution

Cost distribution is out-of-scope of this document: it is discussed in the feasibility study on the implementation of the connections between the eHealth NCPs using the TESTA national networks (activity 3 of the MoU[3]).

III. Gap analysis

In this section, we highlight the shortfall between the current implementation and the target solution; that is, items that have been deliberately omitted, accidentally left out, or not yet defined.

1. Processes

The gap analysis of the process shows that the SMP fulfils most of the requirements, and add new capabilities. Coupled with the SML, it facilitates the configuration management thanks to the dynamic discovery mechanism:

Target solution → / Current implementation ↓	Publishing metadata	Brokered trust	Real-time publication of the configuration	Fetching metadata	Dynamic discovery of new NCP without human intervention*	Removal of the metadata	Eliminated services ↓
Publishing metadata	Gap 1: the SMP must be updated to allow a participant to upload its metadata.						
Brokered trust		Gap 2: the SMP serves metadata signed with its certificate					
Real-time publication of the configuration			No gap: Included				
Fetching metadata				No gap: In the current implementation, the NCPs are selected by configuration. In the target architecture, it is not necessary.			
Logging of all events							Gap 3: the current SMP version doesn't log all the events
New →					New: Dynamic discovery is not possible in the current implementation: each country must be added manually	New: the SMP allows the users to remove their metadata	

Figure 16 - Gap analysis of the processes

*Dynamic discovery of new NCP without human intervention: it is the capability for a NCP-B to discover an unknown NCP-A server without any change in the configuration of the NCP-B.

The gap analysis of the processes shows 3 gaps:

- Gap 1 & Gap 3 are out-of-scope of the SMP specification. DIGIT will implement changes in its reference implementation in order to close the gaps. The severity of these gaps is medium.
- Gap 2 requires a change in the SMP specification. Actions planned to close this gap can be found in section "*3 Open issues*". This gap is critical and is still under discussion.

2. Data

In the "epSOS Change Proposal" from Masi Massimiliano[25], a mapping between the TSL files and the SMP model is described. DIGIT approves this mapping and acknowledges the change requests suggested for the SMP. These change requests have been analysed by DIGIT, discussed with e-SENS experts and are reported in the section "*2 Change requests*" of this document.

[25] epSOS Change Proposal v0.4: CP-epSOS-SMP-v0.4.docx

3. Security

In Chapter 5, "WP5.2 eHealth cross border central services status quo and outlook" concludes that there is no need for a VPN connection between the NCPs and the central services. DIGIT agrees with this conclusion. Therefore, this is the overview of the different interactions between the components:

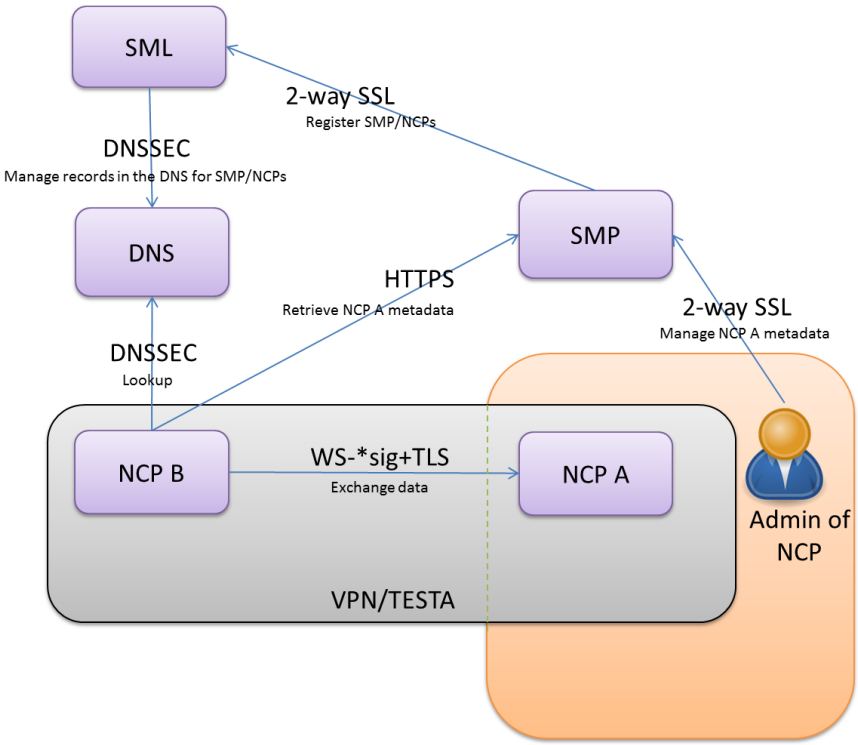

Figure 17 - Overview of the use cases

Note: In section "*II. 3 Replacing the VPN between NCPs* with TESTA-ng", we discussed the feasibility of the replacement of the VPN network with TESTA services. Therefore, depending on the selected option, the NCP components could communicate either over the TESTA network or using the Internet+VPN.

a) Trust zone

For illustration purposes, this section maps the eDelivery components to the eHealth trust zones shown in **Error! Reference source not found.**.

Figure 18 - eHealth Trust Zones

- **SML**, as a central shared component, is hosted by DIGIT. It is hosted outside the national infrastructures, so it corresponds to the **Trust Zone 4**.
- **SMP**
    - In the transitional solution, when the SMP will be used as a central shared component, it will be hosted by DIGIT, therefore in Trust Zone 4.
    - In the target architecture, where the SMP will be a distributed component, it is recommended to be hosted in the trust zone 1, i.e. in the national DMZ. This way, the SMP is protected from the external threats by an internet facing security device that performs packet filtering. Such setup mainly serves to protect availability of the SMP.
- **NCP** gateway will stay in Trust Zone 2.

a) Dedicated PKI trust architecture for eHealth

Figure 19**Error! Reference source not found.** shows eDelivery PKI adapted for the eHealth domain. Root CA (level 1) is the T-Systems root CA, which is publically trusted CA, e.g. trusted by Adobe and by the internet browsers. The sub-CA (level 2) is positioned under the *ec.europa.eu* internet domain, which issues the certificates for NCPs and SMPs (level 3). The intended validity of certificates is 3 years. Note that if the TESTA network is selected as the network layer, the internet domain of the level 2 sub-CA would be *testa.eu.*

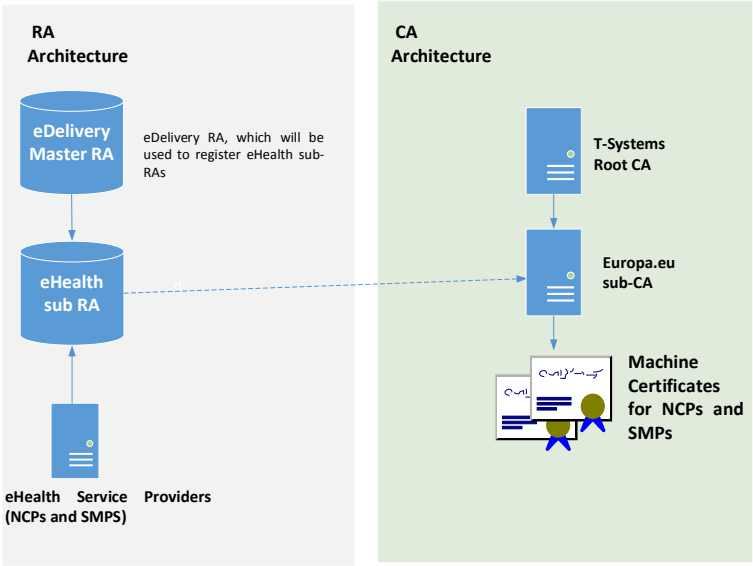

Figure 19 eDelivery PKI for eHealth domain

In what follows, we explain the PKI roles and responsibilities.

1. **eDelivery Master Registration authority (RA)**
   Responsibility: Determination of identity, registration process, revocation of certificates for the domain specific sub-RAs, e.g. eHealth RA.
   Taken by: DIGIT.

2. **eHealth sub-RA**
   Responsibility: Determination of identity, registration process, revocation of certificates for the service providers, i.e. operators if NCPs and SMPs.
   Taken by: DG SANTE.

3. **Certification authority (CA) (T-Systems Root CA, Europa.eu sub-CA)**
   Responsibilities: Certificate management (issue, revocation, renewal), Key management, certificate validation (CRL, OCSP).
   Taken by: T-Systems.
4. **Directory services and online validation (OCSP)**
   Responsibilities: Retrieval of current certificates, Provision of revocation lists (CRLs, ARLs), Online validation (OCSP).
   Taken by: T-Systems.

The following table summarises the split of roles and responsibilities between T-Systems, DIGIT, and eHealth domain.

Process/Service	Responsible Entity		
	T-Systems (PKI Provider)	DIGIT	eHealth Domain (DG SANTE)
CA Setup	X		
Master RA Setup	X		
eHealth sub-RA setup	X		
Domain Registration – Master RA operations		X	
Service Registration-eHealth sub-RA operations			X
Service Initiation - certificate issuance	X		
Service Revocation-initiation			X
Service Revocation-implementation	X		
Certificate and Key Management	X		

Table 5 - PKI Roles and Responsibilities

Creation of a "closed user group" for eHealth domain

In order to provide a "closed user group", i.e. to separate eHealth domain for the other eDelivery domains, e.g., justice or procurement, the naming convention in the certificate metadata is utilised, as shown in Figure 20 below.

NAME ASSIGNMENT (USING AN EXAMPLE OF A USER CERTIFICATE).

- Permitted characters: a-z A-Z 0-9 ' ( ) +, . /: ? = -
- However, character sets are coded in accordance with UTF-8 (O, OU, first name and last name), IA5String (mail) and PrintableString (C)
- Length restrictions for certificate fields
  - Country (C): 2 (in accordance with ISO 3166-1, alpha-2)
  - Name of the organization (O): 64
  - Master domain/client (OU1): 64
  - Area of responsibility (OU2): 64
  - Department (OU3): 64
  - First name (⊆ CN): 64
  - Last name (⊆ CN): 64
  - E-mail (E): 128

Figure 20 Certificate metadata for NCP and SMP certificates

In particular, the following name assignment will be implemented for eHealth domain:

1. **Name of the Organization (O)** has a fixed value: **"DIGIT"**
2. **Master Domain/client (OU1)** can have two values:
    a. **"eDelivery PROD"** for the production certificates;
    b. **"eDelivery TEST"** for the test/acceptance/pilot certificates;
3. **Area of Responsibility (OU2)** has a fixed value: **"eHealth"**
4. **Department (OU3),** can have two values:
    a. **"NCP",** in the certificates issued for the NCPs
    b. **"SMP",** in the certificates issued for the SMPs

A dedicated PKI architecture shown in Figure 19 **Error! Reference source not found.**provides some dvantages compared to the EU TSL based trust, including:

- The NCPs from non-EU countries which are not in scope of the eIDAS trusted lists are able to participate in the network "seamlessly";
- The PKI architecture is aligned with the overall CEF eDelivery architecture, which uses the SML as a central component and it can be trusted by all the participants by sharing the common root CA (ec.europa.eu/testa.eu sub-CA);
- It provides simplified trust validation (e.g. certificate validation), as all the components share the same root CA (ec.europa.eu/testa.eu sub-CA).
- It facilitates the creation and maintenance of the "closed user group", as the domain owner, eHealth, can have a tight control of the NCPs and SMPs authorised to participate in the network.

In the rest of this section, we explain how the trust model based on the EU TSL differs from the PKI based trust.

As shown in **Error! Reference source not found.**, the TSL trust model is based on the fact that the CPs and their services are listed in the national trusted services lists (TSL). When a receiving NCP validates the certificate of the sending one, e.g. for authenticating it for validating its signature, it needs to verify if the originating TSP is listed on the corresponding national TSL.

On the other hand, as shown in Figure 19**Error! Reference source not found.**, the PKI based trust ssumes that NCP certificates are issued under the same root CA (T-Systems CA), which serves as a trust anchor for the participants in the network. When validating a certificate, a receiving NCP builds a certification path, e.g. the list of all intermediate sub-CAs up to the root one. In case the certification path leads to the ec.europa.eu sub-CA (or testa.eu), and that the naming matches the values described in Figure 20, the certificate can be trusted.[26]

In addition to the NCPs, the two other components SMP and SML, are also "certified" under the T-Systems CA and ec.europa.eu sub-CA (or testa.eu), which enables their inclusion on the eHealth trust circle (**Error! Reference source not found.**).

[26] Assuming that all the other checks, such as expiration date and revocation status, are successful.

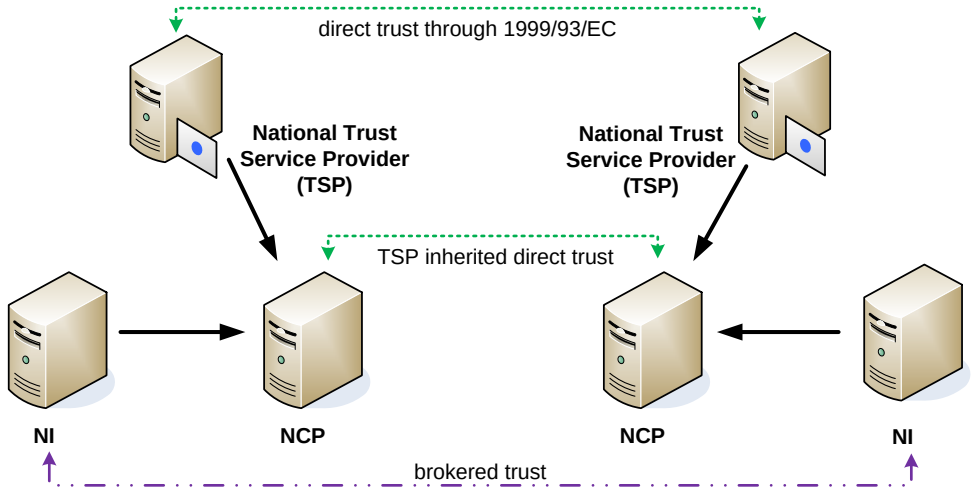

Figure 21 EU TSL based trust

b) List of certificates

Error! Reference source not found. lists all the certificates that are needed to support the trust perations in the eHealth domain, including the certificate type, the registration authority (RA) from which a certificate can be requested and the CA which issues the certificate.

Component	Certificate Type	RA	CA	Comment
NCP	Signing Certificate	eHealth sub-RA	ec.europa.eu Sub-CA	
	TLS Certificate	eHealth sub-RA	ec.europa.eu Sub-CA	
	VPN Gateway Certificate*	eHealth sub-RA	ec.europa.eu Sub-CA	VPN is on the network level, to be checked if it is in scope of the eDelivery PKI. *In case TESTA is selected for the provision of IPSEC encryption, then this certificate is not required
SMP	Signing Certificate	eHealth sub- RA	ec.europa.eu Sub-CA	
	TLS Certificate	eHealth sub-RA	ec.europa.eu Sub-CA	In both transitional and target architecture (SMP central and distributed, respectively).
SML	TLS Certificate	DIGIT	ec.europa.eu Sub-CA	
	Signing Certificate	DIGIT	ec.europa.eu Sub-CA	
DNSSEC	Signing Certificate*	DIGIT	ec.europa.eu	This CA is not

			Sub-CA	online, i.e. it cannot be contacted by the RA and end-users, but will issue DNS certificate to support DNSSEC per domain. *In case TESTA is selected for the provision of IPSEC encryption, then this certificate is not required

Table 6 - Overview of the certificates in the eHealth trust circle

Note: The NCP administrator will use the NCP signing certificate to sign and push the SMP metadata. It is recommended to ensure the secret key does not leave the NCP and that authentication, authorisation and accounting mechanisms are put in place to minimize the risk of compromising NCP signing secret key.

c) PKI trust model - processes

In what follows, we describe the processes that are needed to support the PKI based trust architecture in eHealth domain described in the sections above together with roles and responsibilities of DIGIT, eHealth domain and service providers.

i. Registration of NCPs and SMPs and initiation of a service

The registration of new service providers who operate NCPs and SMPs is initiated through an eHealth sub Registration Authority (eHealth sub-RA), a role established by the eHealth domain. The registration process involves the following steps:

- The National Contact Point (a legal entity) submits an application to the eHealth sub-RAs to operate the NCP and/or SMP services via the established web interface provided by T-Systems. The registration process needs to include submission of all the necessary documentation mandated by the eHealth registration policy. The specific documentation required for the registration in the eHealth domain is out of scope of this document;
- If the service provider is eligible, it signs the contractual agreement with the eHealth domain. This agreement serves to initiate a service by obtaining necessary digital certificates, as explained in the following step;
- A service provider which signed the required contractual agreement with eHealth domain initiates the certificate request; the initiation can be performed via eHealth sub- RA webpage, provided by T-Systems;

0. The requestor generates public/private key pair for each certificate he is requesting (e.g. NCP, SMP). This can done in three ways:[27]
    - Offline, e.g., by using OpenSSL software;
    - Online, by using an online applet offered by T-Systems;
    - By requesting T-Systems to generate the keys on their behalf[28].

[27] Each domain is free to choose a preferred key generation method.

1. The requestor submits the generated public key together with the other required information, e.g. certificate type and intended service (NCP or SMP)[29] in the eHealth sub-RA web portal;
2. eHealth sub-RA sends digitally signed request for certification to the corresponding (sub)CA, which verifies it and issues a signed certificate. The delivered certificates need to fulfil the requirements from recommended certificate profiles defined in D3.A.7 – epSOS EED X.509 Certificate Profiles;
3. The requestor retrieves the public key certificate either via the web portal or via e-mail.

The summary of the registration process is shown in Figure 22 below.

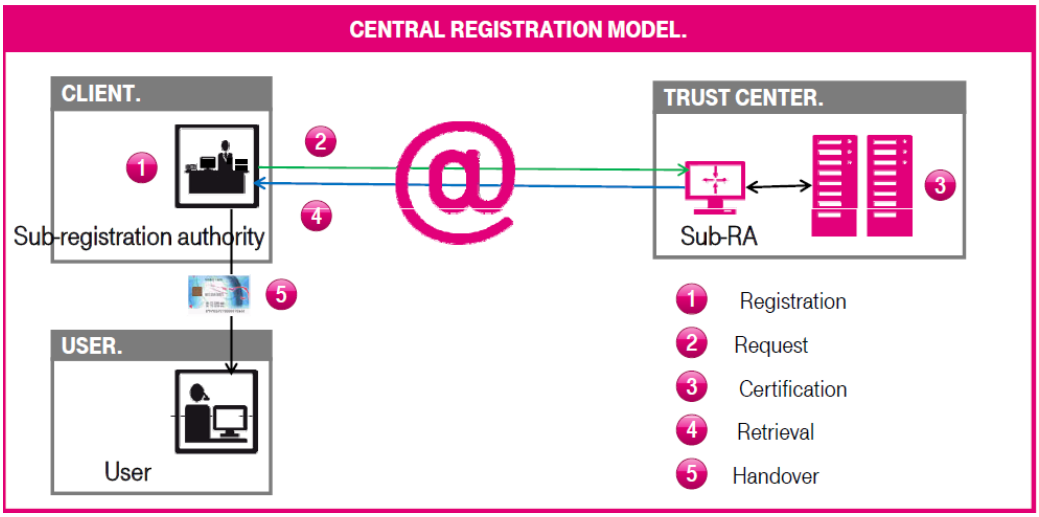

Figure 22 Summary of the certificate request and issuance process

i. Revocation of a service provider

In case a service provider decides to stop participating in eHealth domain, or in case a policy domain owner decides to revoke a service provider for any reason, the corresponding certificate(s) needs to be revoked.

The revocation processes can be described as follows:

- A service provider or a policy domain governing body, e.g., DG SANTE, submits a revocation request to the eHealth sub-RA via the sub-RA web portal;
- The sub-RA passes the revocation request to the sub-CA;
- The sub-CA removes the certificate from the certificate repository and publishes the information in the CRL (Certificate Revocation List) and/or OCSP server.

[28] This would mean that T-System is in position of the private key.
[29] In this step, the certificate requestor will be asked to prove the possession of the secret key corresponding to the submitted public key. This is typically done by signing a value provided by the RA.

IV. Results

1. Conclusions

DIGIT shares the conclusions of the "WP5.2 eHealth cross border central services status quo and outlook[11]" report from e-SENS: SMP/SML is a standard and robust solution that offers benefits to the eHealth domain and allows removing some relaxations introduced in the epSOS LSP.

However, some change requests have been identified. Some of them are out of scope of the SMP specification and will be implemented by DIGIT. Other change requests require modification in the SMP specification and will be submitted by DIGIT to e-SENS in order to make the SMP more generic and more adapted to other domains.

From a technical perspective, moving to the dedicated PKI-based trust model of eDelivery offers some advantages: limited costs, ease of update and common configuration of the PKI services among the NCPs. Also, the migration to the SMP/SML architecture is facilitated because the trust of the centralised components can be inherited from a global root CA.

An evaluation of a dedicated epSOS-PKI was performed in chapter 8.6.2 of the "*D.3.7.2. Final Security Services Specification Definition - Section II - Security Services*[30]". The following concerns were identified:

Concern	Comment from DIGIT
Expensive	The PKI costs of ownership are covered by DG CONNECT.
One NCP or European Node must take it over.	The European Commission takes the responsibility of the PKI
This will imply modifications in the NCPs	We confirm that some modifications are required on the NCP, especially in the SecurityManager.[31] It is important to know that the current implementation doesn't fully comply with the epSOS specifications. Therefore, some other components may also be impacted and refactored.

Of course, migrating to the SMP/SML architecture and/or to the dedicated PKI-based trust model would require changes in the existing epSOS specifications.

To conclude, from a technical perspective, migrating from the trust model of epSOS to the dedicated PKI-based trust model of eDelivery limits the costs and offers limited risks as few components of the NCP are impacted. However, legal factors may restrict the use of the dedicated PKI-based trust model of eDelivery. As stated by Masi MASSIMILIANO in an email of October 7th 2015[32]: "*[…] healthcare is sovereign, and member states (e.g., France) may be mandated to use a national*

[30] D.3.7.2. Final Security Services Specification Definition - Section II - Security Services, http://www.epsos.eu/uploads/tx_epsosfileshare/D3.7.2_epSOS_Final_Security_Services_01.pdf

[32] See ANNEX 5

certification authorities devised for the eHealth. The usage of commercial certificates during the pilot has been a SEG relaxation only."

2. Change requests

These are the change requests regarding the SMP and SML components. They are separated in 2 categories:

- Blocking: Mandatory change for the live implementation and no solution was yet found
- Non-blocking: The change is either:
  - Optional for the live implementation
  - Required but a solution was found

It is important to mention that only REST GET interfaces are defined in the SMP specification. Therefore, any change that has no impact on the GET services won't result in a change in the specification. Changes that impact the specification will result in a "Request for change" that will be submitted to the SMO (Stakeholder Management Office) of CEF, e-SENS and to the OASIS TC committee. DIGIT can modify its sample implementation as long as the change keeps compliance with the specification and as long as the modifications create value for the users.

Internal ID in DIGIT tracking system	Component	Description	Blocking	Impacts the specification	Comment from DIGIT
EDELIVERY-477	SMP	Allow a participant to migrate its data from a SMP to another by himself. ICT-Transport-SML_Service_Specification-101[7] defines a PrepareToMigrate and Migrate call at the SML. This should be also possible at the SMP for users if they migrate their content to another SMP server.	Non-blocking	No	DIGIT believes that the SML MUST only be accessed by the SMP. Therefore, it should not be allowed for a participant to call the migrate or PrepareToMigrate services of the SML. Therefore, the solution is to create a new service "migrate" and prepareToMigrate on the SMP. These services will be responsible to call respective services on the SML and control the credentials and authorisations. This is out of the scope of the SMP specification and don't require any change proposal to OASIS. This will be included in the planning of DIGIT for the development of the SMP with low priority.
EDELIVERY-479	SMP	Use HTTPS instead of HTTP to access SMP for confidentiality reasons	Non-blocking	No	An email was sent on 6th October 2015 to Klaus Vilstrup PERDERSEN (WP6 leader) and Eric GRANDY (e-SENS lead architect). The response of OASIS TC committee is that there is an erratum in the SMP specification. It is actually allowed to use HTTPS as specified in section 3.6.1[33] where it says that *at the transport level an SMP service may either be secured or unsecured depending on the specific requirements and policies of the*

[33] http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/cs01/bdx-smp-v1.0-cs01.html#_Toc407788821

					infrastructure.
EDELIVERY-482	SMP	Change in the metadata in the BDX-SMP specification. TSL has the field "Status" that defines how a given service is acting, e.g., "in Accord", "Reconfiguring", etc. Such record does not exist in SMP, although it can be realised by using ServiceActivationDate. Fields RequireBusinessLevelSignature and MinimumAuthenticationLevel are mandatory for the SMP, but they may have no meanings in other contexts.	Non-blocking	Yes	Until the change request is approved, default values should be used for mandatory fields RequireBusinessLevelSignature and MinimumAuthenticationLevel, and ServiceActivationDate can act as a "status" field.
EDELIVERY-484	SMP	The end records referenced by SMP are documents. A different terminology should be used, because, depending on the domain, end records could be services. The end word "resources" seems appropriate to replace the word "document".	Non-blocking	Yes	To be submitted
EDELIVERY-509	SMP	Log all events on the SMP. The configuration server keeps a trace of all change events, but the SMP doesn't.	Non-blocking	No	This change request was created as a result of the gap analysis of the processes. It doesn't require any change in the SMP specification.
EDELIVERY-486	SMP	Change XMLDSG to aDES	Non-blocking	No	Linked to the decision on EDELIVERY-493.
EDELIVERY-485	SMP	Usage of extension : MUST NOT vs MAY NOT	Non-blocking	Yes	The OASIS TC answered with an agreement in principle[34]: "*The TC recognises that agreements of use of extensions within a community should not hinder the application of the SMP specification as you intend. We also recognise that a clarification would help this understanding and we are in the process to issue a TC committee note to ensure clarification. You can go ahead as planned and the Committee Note will be issued for later reference."*
EDELIVERY-505	SMP	Allow users with less than administrative permissions to manage their own metadata	Non-blocking	No	DIGIT proposes 2-way SSL authentication between the user and the SMP for all the PUT/DELETE services. The SMP will manage internally the list of authorised users.
EDELIVERY-493	SMP	SignedServiceMetadata records to be signed with a Participant certificate instead of the SMP certificate	Non-blocking	Yes	On 15/10/2015, a meeting was held between DG-SANTE, DIGIT and e-SENS. It resulted in a 3-solution plan: 1) Add the SMP as trusted node in the epSOS network. Due to the legal complexity of the FwA, all the MS should agree on this point. The

[34] http://gazelle.ihe.net/jira/browse/EPSOSMAINT-7

					implications are that the SMP will inherit the trust zone of the NCPs. 2) Use multiple signatures (the first signature is from the Scheme Operator, the Second is for SMP). This will not affect the epSOS trust model, but it violates with the SMP specifications. The implication is for OASIS to discuss in their TC how to change the specifications. 3) Use the extension: the SMP receives a ServiceMetadata signed by the scheme operator. It moves this signature to the extensions element, and signs it as per SMP workflow. The client verifies the signature of the SMP, and the NCP performs again a signature using the Signature element of the extension. We can try to address #1 and #2 in parallel and leave option #3 as a fallback solution if #1 or #2 fail.
EDELIVERY-506	SML	Assess the DIGIT's implementation of the SML for readiness to multiple domain support. Assess the capabilities of the new SML for the following features: configuration of DNSSEC per domain, possibility to enable/disable DNSSEC per domain, authorisation and authentication per domain	Non-blocking	No	This requirement is not specific to eHealth and doesn't have an impact on SML and BDXL specifications.

3. Open issues and questions

ID	Description	Comment
1	DIGIT doesn't provide DNSSEC services	SNET plans the deployment of DNSSEC services for the first semester 2016[35]
2	Evaluate if the participating nations would agree to migrate to the dedicated eDelivery PKI	
3	DIGIT to ask SNET to confirm that the centralised SMP, SML and DNS can be available on the TESTA network	

[35] Response received on 12/11/2015 from SNET for the SMT-ES ticket number "IM0014027851"

V. Migration plan

The scope of the migration plan is to illustrate the activities that need to be conducted in order to reach the second phase where all Participating Nations can start using the centralised SMP and SML components. Prior to the second phase is the first phase. As described in chapter "*II Target solution*", during the first phase a centralised SMP is deployed. During this phase, only a set of selected and voluntary Participating Nations migrate their configuration to the centralised SMP. According to the migration plan, this would start in August 2016 using an acceptance environment hosted by DIGIT.

The first phase is finished when all the selected countries have moved their metadata to the centralised SMP and when the migration process is approved. Of course, the conclusion of the first phase is subject to the Participating Nations availability constraints.

In September 2016, the second phase should begin, and all the Participating Nations would start using the centralised components hosted at DIGIT in a production environment.

During the EXPANDATHON, the "SMP integration profile" was successfully run by 5 PNs[36]. The results and the lessons learned from the EXPANDATHON will allow DG SANTE and the OpenNCP community to start the adaptation of the OpenNCP as from January 2015. Because the PUT interfaces won't yet be agreed at this time, the integration will only concern the GET interfaces of the SMP.

[36] http://gazelle.ihe.net/EU-CAT/testing/results/connectathonResults.seam?integrationProfileOption=1&testSession=34&integrationProfile=388&sort.id=ascending

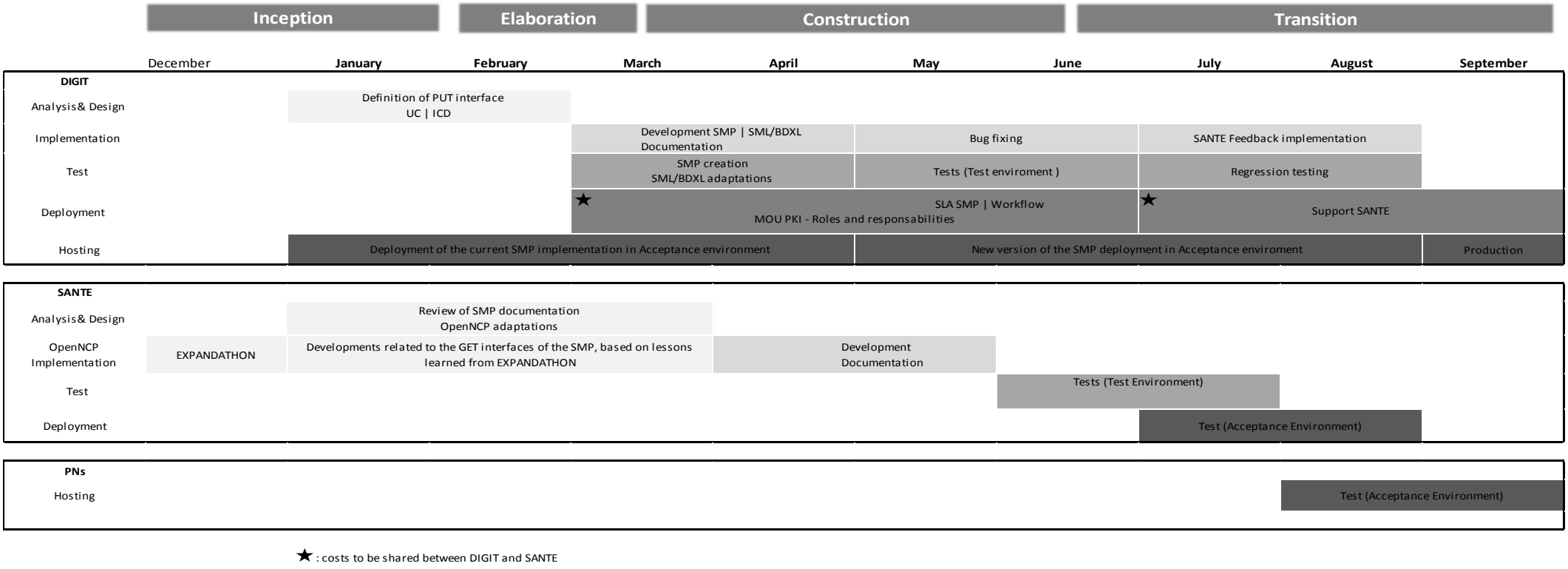

Figure 23 - Migration plan from the first phase up to the second phase

For DIGIT, the total effort estimation for the migration plan is 425 man days. The cost will be mainly supported by DIGIT but 3 deployment tasks, for a total of 120 man days, are specific to the eHealth domain and will be shared between DIGIT and SANTE:

- SLA SMP / Workflow
- MoU PKI – Roles and responsibilities
- Support SANTE

Task	Profile	Effort Estimation (man days)
Definition of PUT interface	SMP/SML Expert	20
	Business Analyst	40
Development SMP | SML/BDXL Documentation	Business Analyst	20
	Developer	40
	SMP/SML Expert	40
SMP creation SML/BDXL adaptations	Tester	40
Bug fixing	Developer	20
Tests (Test enviroment)	Tester	20
SLA SMP | Workflow ★ MOU PKI - Roles and responsabilities	Business Analyst	80
SANTE Feedback implementation	Developer	10
Regression testing	Tester	10
Support SANTE ★	Support	40
Project Management	Project Manager	45
	Total	425

★ : costs to be shared between DIGIT and SANTE

Figure 24 - Effort estimation per task

ANNEX 1

Minutes of our talk from yesterday.msg [37]

ANNEX 2

Meeting minutes - Configuration server [37]

ANNEX 3

Minutes meeting - SMP SML integration [37]

ANNEX 4

SMP SML infos OpenNCP.msg [37]

ANNEX 5

RE Antwort RE OpenNCP SMP SML T… [37]

[37] The contents of the emails are only available in the Word version of this document