**COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME**

**ICT Policy Support Programme (ICT PSP)**



Project acronym: e-SENS

Project full title: Electronic Simple European Networked Services

ICT PSP call identifier: CIP-ICT-PSP-2012-6

ICT PSP main theme identifier: CIP-ICT-PSP-2012-6-4.1 Basic Cross Sector Services

Grant agreement n°: 325211

5.2 eHealth cross border central services status quo and outlook

|  |  |
| --- | --- |
|  |  |
|  |  |
| Version : | 0.2 |
| Status : | – INTERNAL – Draft |
| Dissemination Level : | Confidential in Commerce |
| Work Package : | 5.2 |
| Organisation name of lead partner for this deliverable | SPMS, LIST |
| Author(s): | João Gonçalves (SPMS)  Uwe Roth (LISt |
|  |  |
|  |  |
|  |  |

Abstract:

Provides an overview of the epSOS/EXPAND Central Services and a suitability analysis of the WP5.2 SMP/SML.

Table of Contents

1. Introduction 3

2. epSOS Central Services security specification 4

2.1. Proposed solution 4

2.2. Security and Trust 6

2.2.1. epSOS Trust model 6

2.2.2. epSOS Trusted Service List 8

2.2.3. Trust Service Providers 9

2.2.4. Security protocols and messaging 10

2.2.5. Cryptographic keys and algorithms 11

2.2.6. Certificates 12

2.2.7. ATNA Secure Node 13

2.2.8. Audit 13

3. epSOS Central Services security relaxation specification and implementation 14

4. SMP/SML OpenNCP implementation specification 17

5. Security and sustainability analysis 18

5.1. DNSSEC, DANE, RPKI 18

5.1.1. DNSSEC 18

5.1.2. DANE 18

5.1.3. RPKI 18

5.2. TSL File 19

5.3. Privacy concerns 19

5.4. Provision of TSL Information via SML/SMP 20

5.5. Upload of Information to the SMP 21

5.6. Pros and Cons for the use of the SML/SMP standard 21

5.7. End-to-End-Encryption and the use of VPN 22

5.8. Use of the TSL Information for VPN 22

6. Recommendations / Roadmap / Conclusions 24

# Introduction

epSOS provided a set of deliverables that stipulated the legal, organisational and technical requirements needed to be fulfilled by nations adopting the NCP to provide eHealth cross-border services. Even so, some of the requirements were relaxed in order to ease the beginning of the pilots, specifically regarding the Central Services, a mechanism used by the nations to share configurations of their NCP. In order to remove some (or all) of those relaxations, e-SENS is pushing into the eHealth domain a building block based on service metadata: SMP/SML.

As such, a requirement gathering and impact assessment on the introduction of this new component in the OpenNCP architecture is needed, to understand how it will help to close the gap between the specifications and the implementation.

This document focuses on the eHealth needs regarding the new approach on the OpenNCP configuration: SMP/SML. First, it is provided a view on the Central Services specifications and functionalities regarding configuration files, in a TO-BE and AS-IS point of view. It then proceeds to analyse the requirements of the new SMP/SML specification and its implementation as a new building block in OpenNCP, migrating from the current Central Services. A gap analysis will provide a clear understanding of advantages/disadvantages and how the new solution could evolve to best fit the eHealth domain requirements.

# epSOS Central Services security specification

This section describes the specifications developed for the epSOS Central Services.

## Proposed solution

The need for the Central Services comes from the fact that every NCP must be an ATNA Secure Node[[1]](#footnote-1), that is, no administration access to the machine is allowed. Therefore, the configuration of the environment should be automated. The Central Services maintain the data that is distributed to each NCP and thereby used in the business transactions. The objective of central services is to create, maintain and share common data in a secure and efficient manner. Some of this common data is specific for each NCP and public to all other NCPs and it can be classified as:

* Trust anchors;
* End point addresses, VPN, NCP, IdP and HCP certificates (in TSL);
* MS policies & documents:
  1. (Patient)information paper (D2.1);
  2. Confirmation requirement policy (D3.6);
  3. HCP allowed roles (D3.6);
  4. NCP PS eP data hiding disclaimer (D3.4.1).

The specification divides the services into two types:

* Central services: services with a single distribution point, used for terminology management (eCRTS);
* Shared services: also called "virtual central services", which have a distribution point per NCP.

As the terminologies are out of the scope of this document, we'll focus on the "virtual central services", which keep the common data previously listed.

The proposed solution for these central services (D3.9.1 § 5 – Central Services)[[2]](#footnote-2) is based on DNS and HTTP distribution: each country would maintain an HTTP-service on its NCP that would provide its documents in its responsibility, using a convention for the naming scheme. The DNS would order the requested DNS name for the proper MS NCP. Each NCP would have its data organized in two virtual versions (structures): Drop-zone ("drop", representing the TO-BE status) and Running Configuration ("running", representing the AS-IS status). These structures should be exposed as REST resources and group information related to configuration files and terminologies:

There should be a SubVersioned structure for this information to be placed in order to provide full traceability.

/centralservices/<version>/

/centralservices/<version>/organisation/

/centralservices/<version>/organisation/contacts.pdf

/centralservices/<version>/NSL/\*.TSL (D3.4.2)

/centralservices/<version>/MTC/... (Semantic Expertise Group)

/centralservices/<version>/MVC/... (Semantic Expertise Group)

The name standard would follow the pattern:

https://<country-code>.epsos.eu/centralservices/<version>/<hierarchy>.../<document>

Figure 1 depicts the described scenario.

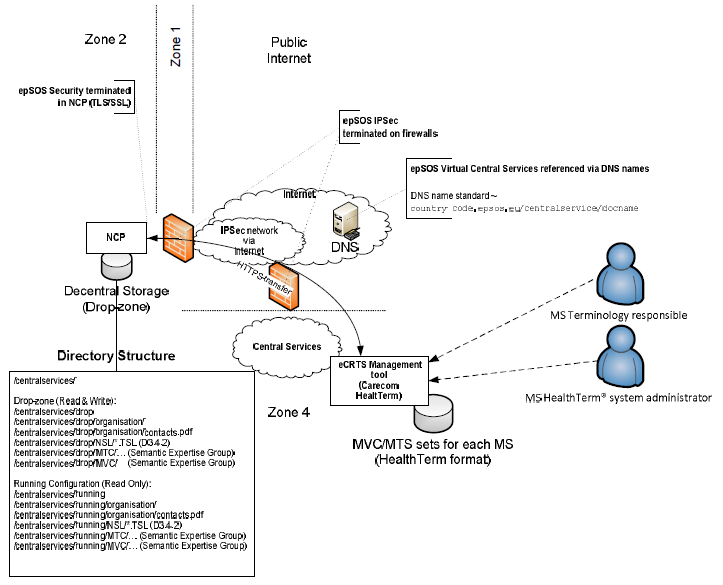


Figure 1 - Virtual Central Services - proposed solution

For this scenario, the following configurations would be needed by the NCPs:

|  |  |  |
| --- | --- | --- |
| **Key (Configuration item ID)** | | **Description of configuration value** |
| Local.CentralServices | | Path where local copies of configuration data is stored. The default value is "%epsos%/centralservices" |
| Local.NslDropZone | | Path where the NCP's own NSL is maintained. The default value is "%Local.CentralServices%/drop/NSL" |
| Local.NslRunningZone | | Path where the current version of the NCP's NSL is available for access by other NCPs. The default value is "%Local.CentralServices%/running/NSL" |
| CoT.CountryCodes | | Semicolon-separated list of all countries that are in the same circle of trust as the NCP. Example: "dk;se" |
| Local.LanguageCodes | | NCP-supported language codes (ISO 639-1). PoC Registration Data for multi-lingual MS |
| Configuration for each connected NCP / country (zz is short country-code) | ZZ.nsl.URL | URL of the Austrian, German, Danish, etc. NSL. Example: https://countrycode.epsos.eu/centralservices/running/nsl/nsl.tsl |
| ZZ.OrderService.WSE  ZZ.PatientService.WSE  ZZ.DispensationService.WSE  ZZ.ConsentServce.WSE | Webservice endpoints of the national epSOS WSE are taken from the countries' NSLs Synchronizer and written into the configuration. The entries MUST NOT be managed manually. |

Table 1 - NCPs configuration properties

## Security and Trust

### epSOS Trust model

epSOS does not establish direct end-to-end trust relationships between data producers and data consumers. Instead epSOS security relies on a “brokered trust” (direct brokered trust) paradigm where NCPs act as trust brokers between a national infrastructure (NI) and the epSOS domain. NCPs are bound to the epSOS trust domains as well as to their national trust domain. As such they are assumed as trusted by other NCPs and by all services and actors within their respective national infrastructure (D3.A.7 epSOS X.509 Certificate Profiles § 1 – Use of Public Key Security in epSOS)[[3]](#footnote-3).

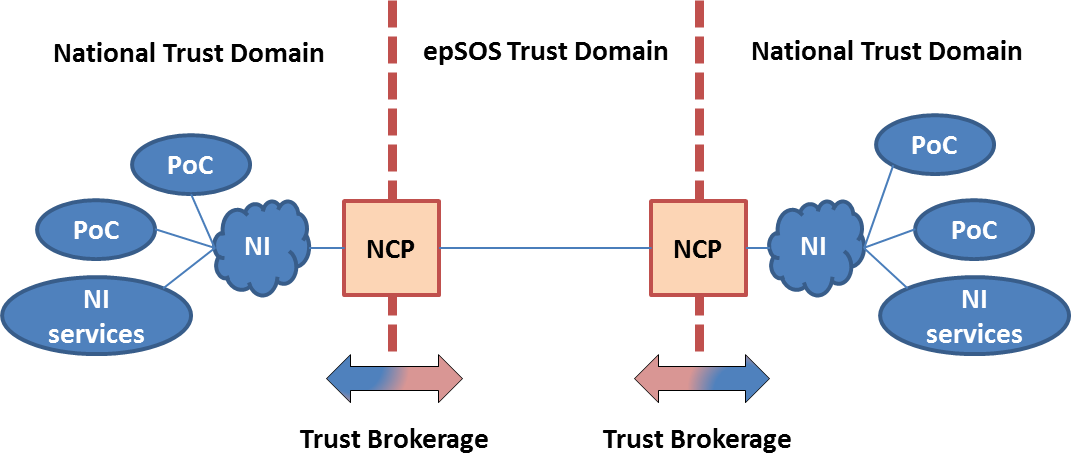


Figure 2 - epSOS trust model

Another point of view on this subject is the one provided by the ISO27000 concept of protection rings (security zones).



Figure 3 - epSOS security zones

According to Massimiliano Masi’s draft document on the trust model for the eHealth domain[[4]](#footnote-4), the following explains how the different zones coexist in order to implement the direct brokered trust paradigm:

* The first zone is formed by the whole internal network of a country. Basic security measures (packet filters and a dedicated internal network infrastructure) protect it from outside threats;
* The second trust zone is formed by a subset of the first zone. Internal security measures like a logical and physical separated network that is only accessible through a gateway protect the environment even from internal threats. For epSOS applications epSOS-NCP gateways act as the only entry and exit point from this zone;
* Trust zone III is a subset of trust zone II. In addition to the measures that are in place to secure the second zone, additional protection is provided. This trust zone corresponds to the existing national eHealth infrastructures which are considered to be secure by definition;
* All common epSOS directories and services (e. g. for reporting and management) are located in a separated trust zone (four);
* National Infrastructures have a direct trust with their NCPs, which trust themselves.

### epSOS Trusted Service List

NCP Service Status List (NSL) files are used to convey information on network addresses, web service endpoints and certificates of a country's service providers and consumers. These files are signed by a trusted authority of the respective country. NSL files are encoded as ETSI Trust-service Status List (TSL) acc to [ETSI TS 102 321][[5]](#footnote-5) and must be available as XML files. They should also be available in a human-readable PDF/A format. Figure 4 shows the information that the NSL file has the capability to accommodate:

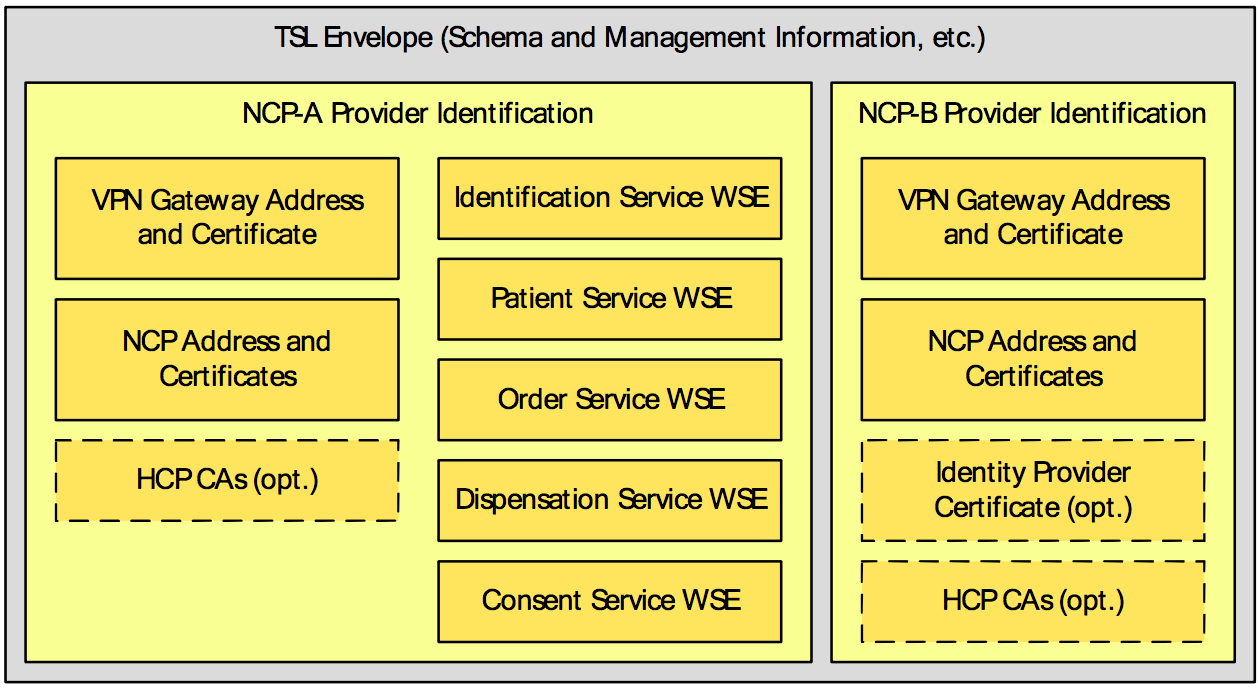
So, for each face of the NCP (NCP-A and NCP-B), a country can provide information regarding:

Figure 4 - ETSI TSL for encoding epSOS service status information

* VPN gateways: address and digital certificate;
* NCP gateways: web service endpoints, certificates for authentication and message signatures;
* Identity Provider: information and certificate of country-B’s dedicated Identity Provider.

Table 2 shows which of this information is mandatory (M) or optional (O) for NCP-A and NCP-B:

|  |  |  |
| --- | --- | --- |
| **Gateway / Service** | **NCP-A** | **NCP-B** |
| epSOS VPN Gateway | M | M |
| epSOS NCP | M | M |
| epSOS Patient Identification Service | M | - |
| epSOS Patient Service | O | - |
| epSOS Order Service | O | - |
| epSOS Dispensation Service | O | - |
| epSOS Consent Service | O | - |
| HCP Identity Provider | - | O |
| HCP Signature CA | O | O |

Table 2 - epSOS mandatory information for NSL files

The complete TSL structure and its usage for the epSOS use case is described with more detail in epSOS deliverable D3.4.2 § 4.4 - epSOS Trusted Service List[[6]](#footnote-6).

### Trust Service Providers

In order to establish the epSOS trust bootstrap, TSL files published by each nation should be signed/accredited by a nation’s trust anchor: the National Trust Service Provider (TSP). Directive 1999/93/EC stipulates that there is direct trust between TSPs from different nations. NCPs are not automatically considered trustworthy but inherit their specific trustworthiness from their appointed authoritative national TSP. Therefore, the anchor of any trust relationship between epSOS PNs is implemented through the appointed national TSP: the PNs do not immediately trust any foreign NCP per se but the TSP of the other PNs. All information within an epSOS TSL envelope is integrity and authenticity safeguarded by applying suitable technical means to the TSL through a PN-appointed TSP (D3.A.3 § 6.2 – epSOS Node and Service Discovery)[[7]](#footnote-7).



Figure 5 - TSP-enabled trust model

### Security protocols and messaging

epSOS uses a layered communication infrastructure that separates the different concerns and requirements of the legitimate data exchanges (D3.A.7 epSOS Messaging Profile § 1 - Introduction)[[8]](#footnote-8).

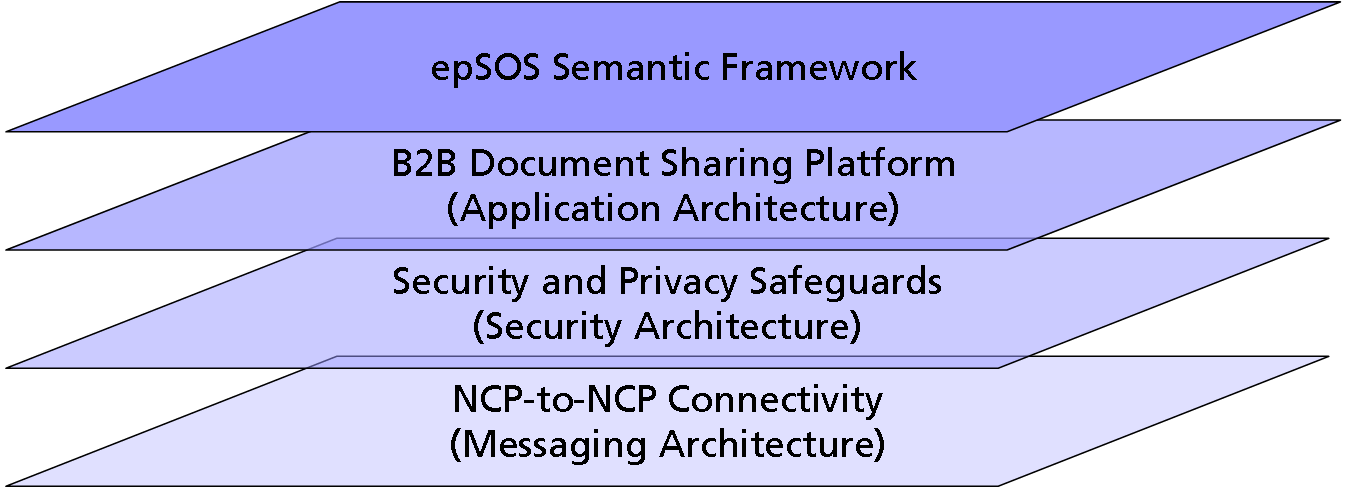


Figure 6 - epSOS 4-layer Architecture

All exposed exchanges are audience restricted through confinement by:

* epSOS virtual private network (IPSec VPN [RFC 4301][[9]](#footnote-9)) on top of the public internet;
* Message encryption (TLS v1.0 [RFC 2246][[10]](#footnote-10)) and integrity protection;
* IHE Audit Trail and Node Authentication [IHE ITI TF-2a][[11]](#footnote-11) (mutual NCP authentication).

These are the means used to establish the mutual trust between nodes and create the epSOS trusted node infrastructure that implements the core epSOS security services to ensure the confidentiality of medical data transmission and the availability and authenticity of epSOS services. It must be noted that only NCPs acting as epSOS service providers and consumers are part of the epSOS trusted node infrastructure as specified in this document. Points of Care within country B or national data registries/repositories in country A have to be connected to the epSOS trusted nodes by means that respect the epSOS end-to-end privacy, security and data protection requirements (D3.4.2 § 4 – epSOS Communication and Messaging Infrastructure).

The epSOS NCP-to-NCP Connectivity layer spans a private communication network among NCPs and provides functionalities for epSOS service discovery. It links epSOS Central Services to the epSOS network and provides means for synchronizing local NCP configuration data from epSOS Trusted Service Lists and globally managed terminologies (D3.A.3 § 2.5.1 – epSOS 4-layered Architecture).

According to D3.4.2 § 4.1.1 - IPSec Configuration, a gateway-to-gateway VPN must be set up between all epSOS nodes. IPSec ESP transport modus must be used. Perfect Forwarding Secrecy must be activated. SA Lifetime should be based on the number of exchanged packets and should not exceed 4GB. Algorithms and key lengths must be used acc. to section 2.2.5 of this document. Gateway certificates must comply with the certificate profiles as defined in section 2.2.6 of this document. The issuing CAs and all components and services for managing the lifecycle of the certificates must comply with the respective epSOS security policies (D3.7.2[[12]](#footnote-12)).

### Cryptographic keys and algorithms

All cryptographic keys and algorithms used for epSOS and its implementations must fulfil at least the requirements of [ECRYPT-II D.SPA.57][[13]](#footnote-13) for Level-5 (Legacy Standard) security. This corresponds to 96-bit security (symmetric equivalent). The use of the 112-bit equivalent Level-6 (Medium Term Protection) security is recommended (should) for message security. The use of the 128-bit equivalent Level-7 (Long Term Protection) security is recommended (should) for data security and digital certificates.

[ECRYPT-II D.SPA.57] recommendations define the epSOS minimum requirements on the selection of cryptographic keys and algorithms. Countries participating in and epSOS circle of trust may agree to choose another algorithm catalogue (e. g. [BSI TR-3116][[14]](#footnote-14), [FNISA CryptMech][[15]](#footnote-15), [NIST SP800.57/1][[16]](#footnote-16)) as long as this does not fall behind [ECRYPT-II D.SPA.57] level-5.

Algorithms based on elliptic curves may be used if agreed by all countries that participate in the respective circle of trust. If SHA-2 is used, only non-patented hash algorithms of the SHA-2 family must be used (recommendation: SHA-256 (should)). SHA-1 may be used as a hash algorithm for the epSOS pilots, but a country may react to respective messages and security token with an error requesting SHA-2 to be used (D3.4.2 § 5.1 – Cryptographic Keys and Algorithms).

### Certificates

epSOS security mechanisms build upon SAML assertions and digital certificates as core security objects that allow the implementation of the epSOS trust model. This section provides the respective epSOS security object profiles on X.509 certificates that are used for public key security within epSOS.

Public key infrastructures (PKI) are based on the ITU-T X.509 standard that specifies formats for public key certificates, certificate revocation lists (CRL), attribute certificates, and means for certification path validation. Common epSOS certificate profiles ensure an equal level of trust among all epSOS participating nations and are prerequisite to a common understanding of the key characteristics of trustworthy certificates within the epSOS network. Deliverable D3.A.7 epSOS X.509 Certificate Profiles § 2 – General Considerations provides some of the requirements related to certificates.

#### Pilot Tests vs Operations

epSOS participating nations may use different certificates for epSOS pilot testing and epSOS operations. Security relaxations may be applied to testing certificates and must not be applied to operational certificates. Operational certificates may be used for pilot testing. Pilot testing certificates must not be used for epSOS operations.

#### Algorithms and key length

All cryptographic objects and algorithms contained with epSOS compliant certificates must follow the guidelines stated in section 2.2.5.

#### Certificate Issuing Authorities

All certificates used for epSOS operations must be issued by a trustworthy authority that is registered with an epSOS PN Trust Service Status List [ETSI TS 102 231].

#### Certificate Verification

Each certificate that is received by an NCP as part of a security handshake or within a digital signature must be verified by that NCP. The following verifications apply to both piloting and operational certificates:

* The current date must be within the validity range of the certificate;
* The certificate must not be revoked;
* Algorithms and key length must comply with section 2.2.5.

The following verifications must be applied to operational certificates and may be omitted for piloting certificates:

* The certificate itself or a certificate within the certificate’s certificate chain must be registered within an epSOS Trusted Service List;
* The use of the certificate must be compliant with its key usage element as specified for the respective certificate profile (section 2.2.6.5).

#### Certificate Profiles

The epSOS certificate profiles are completely described in D3.4.2 § 5.4 – epSOS Certificate Profiles.

### ATNA Secure Node

All network nodes running epSOS service consumers or service providers MUST be implemented as IHE Secure Node actors acc. to the IHE ATNA profile. The establishment of mutual trust and the setup of the secure transport layer channel between two epSOS nodes are always initiated by a service consumer that connects to a service provider. The messages for the establishment of the basic transport layer secure channel correspond to the TLS handshake protocol as profiled in the IHE ATNA Integration profile (transaction ITI-19 as specified in section 3.19 of [IHE ITI TF 2a]). With respect to the ITI-19 transaction specification the following constraints and extensions apply:

* Algorithms and key lengths must be used acc. to section 2.2.5 of this document;
* The node certificates must comply with the epSOS Node Authentication Certificate Profile (see section 2.2.6 for the certificate profile specifications);
* The issuing CA and all components and services for managing the lifecycle of the epSOS Node Authentication Certificates must comply with the respective epSOS security policies (D3.7.2).

### Audit

According to D3.4.2 § 4.5.7.3 – Import of an epSOS NCP Trusted Service List, an NCP must write an audit trail entry for the import of another NCPs Trusted Service List. The audit message must be assembled according to the HCP Assurance audit schema as defined in D3.4.2 § 4.5.3 – epSOS HCP Assurance Audit Schema.

# epSOS Central Services security relaxation specification and implementation

After studying the specifications, the task force assigned to this assessment had to take a look at the current implementation of the central services in order to understand how much of it conforms to the specification and identify the gaps (relaxations) that exist. For that, it was asked help to the current central services provider, CONET, and team’s contact point was able to provide valuable information that no one in the community had, which will be summarized in the following paragraphs.

The first thing that should be noticed is that the proposed solution for the central services, explained in section 2.1 was never implemented. The closest description to that currently exists is provided by Massimiliano Masi and Rainer Hörbe's draft document “NCP configuration files & epSOS central services specification”[[17]](#footnote-17) and Massimiliano Masi’s webinar. [[18]](#footnote-18)

CONET is responsible for the server and provision of services that enable the upload of the TSL files to the central services. The current workflow of distributing the TSL files follows a publish-subscribe model where each country uploads its TSL file to the central services repository and decides (in its own NCP configuration) which countries’ TSL files it want to download from the central services.

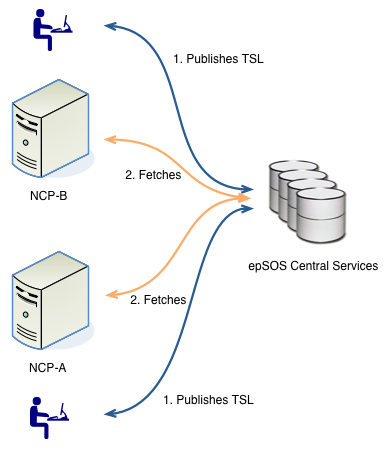


Figure 7 - TSL publish-subscribe workflow

A country connects to CONET’s server by using a confidential and mutually authenticated protocol (SFTP), to enforce confidentiality, integrity and non-repudiation, providing its username and public SSH key. If the Public-SSH-Keyfile for this country is correct, they are able to upload a file in their home directory (a private directory that each country has: DropZone). On the server runs a script (which was provided by the provider before CONET) that checks some parts and if all checks are OK the file will be uploaded from the home-directory into the webserver (publicly available directory: ConfigArea) and the file is ready for download. During this process, an audit log is produced and saved. CONET provides this files on the following addresses:

* PPT: https://ecrtsppt.conet-services.de:8445
* Production: https://ecrts.conet-services.de:8445

The directory structure for the private area of each country follows the pattern (<CCC> - 3-letter country code, e.g., AUT for Austria, GRE for Greece, etc):

* PPT: /sftp/<CCC>/PPT
* Production: /sftp/<CCC>/

In OpenNCP, the TSL Editor is the GUI tool responsible for aiding in the creation and upload of the TSL file to the central services. In order to download the file, each NCP node needs to run TSL Sync, which will authenticate the TSL, check its integrity and update the internal configurations, writing an audit trail. The following figure provides a clear view on this scenario.

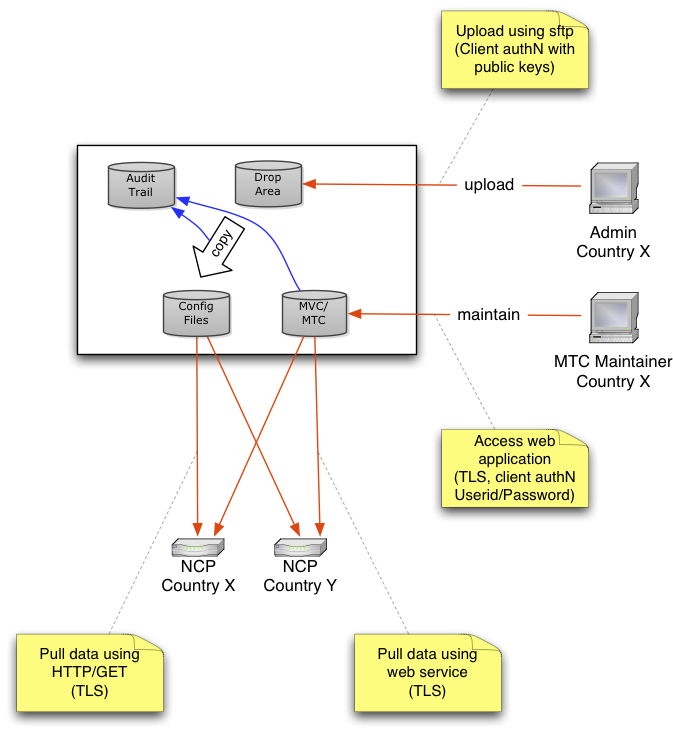


Figure 8 - TSL workflow

This is the workflow the former provider implemented and that CONET copied to their server.

On the referred draft documents, it was noted that the private area of each country would contain more than just the TSL files. In fact, some countries had some files stored there but CONET is not responsible for them. For instance, the files for Luxembourg are a bit out-dated (2013). In the public area, files for some (but not all) of the international search masks could be found, but also dated of 2013.

Regarding the VPN connection from each NCP to the central services, CONET stated that there was a plan to implement, it was tested with Luxembourg but it was never implemented in Production.

The central services’ internal script was provided to the OpenNCP team and is now being studied in order to shed some more light on this topic.

After gathering all this knowledge, the team could identify some relaxations introduced:

1. Certificate profiles

* For pilot testing several security relaxations may be applied to epSOS certificates which are used during pilot testing. Relaxations must not be applied to certificates which are used for epSOS operations. (D3.A.7 – epSOS EED x509)
* Although the normative specification mandatorily specifies the usage of SHA-2 hash algorithms, many PN were unable to obtain compliant certificates on short notice or the foreseeable future. Furthermore, some PN are also unable to obtain a compliant set of certificates from a Trusted Third Party provider due to organisational constraints. Consequently, the provision of compliant and harmonised certificates for all epSOS PN that plan to pilot was unsuccessful with the certificate issue being a blocking factor. As a compromise, WP 3.10 and TPM authorised the temporary use of SHA-1 certificates until the end of 2012 under the condition of a thorough assessment by epSOS security experts and the PSB Legal Expert Group (PSB-LEG). Agreed Relaxation: SHA-1 MAY be used as a hash algorithm for the epSOS pilots until the end of 2012, but a country MAY react to respective messages and security token with an error requesting SHA-2 to be used. (D3.A.7\_epSOS\_EED\_Algorithms-and-Key-Length\_v1.0-2)

1. Lack of VPN connection between central services and NCPs
2. NCPs are not ATNA Secure Nodes

* OpenNCP doesn’t not provide a component like F.E.T.’s SyncApp that acts like a scheduled synchronizer that runs TSL Sync and automatically updates the configurations of the NCP. OpenNCP requires manual running of the TSL Sync.

1. epSOS trust bootstrap has been relaxed by using the mutually-acknowledged TSL file

* There are no TSPs as far as we know

# SMP/SML OpenNCP implementation specification

# Security and sustainability analysis

## DNSSEC, DANE, RPKI

### DNSSEC

The SML/SMP standard bases on the use of DNS to store the link to the SMP in a special Meta:SMP record of the domain that is hosting this machine. Initially, DNS records are not trustworthy and can be changed and manipulated, e.g., by DNS cache poisoning. DNSSEC addresses this problem by the use of signatures of zone information. With this, the authenticity of DNS records can be proven.

### DANE

DANE is an extension of the DNSSEC standard. It addresses the problem that certification authorities in the past had created certificates for domains that are not owned by the certificate-requestor (e.g. certificates of google.com, yahoo.com). With the DANE standard, the user of a secure protocol like TLS can prove (by checking the TLSA record in the DNS), that the certificate that is being used in the communication is really the one that should be used for that domain.

### RPKI

Newest findings[[19]](#footnote-19) have shown that not only the DNS content must be secured with DNSSEC, but also routers are potential targets of attacks. If someone is able to control a BGP-router (BGP=Border Gateway Protocol), he or she is able to add routes that usually don't fall in the IP-range that the router manages. Other BGP routers that communicate with the hacked router via BGP are not able to check such information. Traffic of the given IP range will then be routed to the wrong systems.

If the attacker then requests an SSL certificate of a domain that falls into the occupied IP rage, the certification authority checks the ownership of the domain by accessing a special HTTP page. Since the traffic will be re-directed, the CA finds all necessary information on the server of the attacker and creates the desired certificate.

A solution to avoid such attacks is the use of RPKI (Resource Public Key Infrastructure), that links the systems with a trustworthy remote station (trust anchor) on base of X.509 certificates. With such a certificate, a trust anchor confirms - towards a requesting BPG router - that another router is responsible for a certain IP range. Unfortunately only 0.76% of all IP ranges are protected via RPKI.

In our context we should ensure that this technique is also used in all controlled BGP routers.

## TSL File

epSOS Architecture and Design EED DESIGN – epSOS TSL Profile[[20]](#footnote-20) describe the structure of TSL files and the way these files are synchronized between several countries. A simplified version about this can also be found on Fraunhofers epSOS wiki[[21]](#footnote-21),[[22]](#footnote-22). The document is titled as a draft version that needs validation, but from our knowledge, it describes the current state of implementation. No newer version is available that is defined as final.

A TSL file is an XML file that contains the following information as shown in Figure 4 - ETSI TSL for encoding epSOS service status information.

There are finally two questions about this content regarding the migration to a SML/SMP based solution: Does it contain private information and is it possible to make such information in an SML/SMP based available?

## Privacy concerns

The following table lists all relevant data that is stored inside a TSL file.

|  |  |  |  |
| --- | --- | --- | --- |
| Data | Function | Privacy evaluation | Could be public? |
| Management Information | Here the TSL file gives information contact information of the operator, including eMail-address, postal address. | This is not private information. Similar information as in the DNS server for technical contact. EMail and postal-address are from the organisation and not from the private person. | yes |
| Service IP addresses | Public IP address of the service | Not publishing the IP address does not mean, that it cannot be accessed or be the target of a denial of service attack.  Access to the machine behind the IP address is only possible from machines that are able to create the VPN tunnel to the VPN gateway plus being permitted in the firewall to access the relevant ports in on the end-system. | yes |
| VPN Gateway Certificate | Public certificate of the VPN Gateway | The purpose of public certificates is, that they are public. No information in the certificate should be kept secret. | yes |
| NPC TSL Certificate | Public certificate used for encryption | The purpose of public certificates is, that they are public. No information in the certificate should be kept secret. | yes |
| NPC Signature Certificate | Public certificate used for proof the signature of a document | The purpose of public certificates is, that they are public. No information in the certificate should be kept secret. | yes |
| HCP CAs | Optional certificate of the CA of the HCP | The purpose of public certificates is, that they are public. No information in the certificate should be kept secret. | yes |

From the authors’ point of view, the TSL file does not provide any information that only should be kept inside the circle of trustworthy domains.

## Provision of TSL Information via SML/SMP

In the draft document from Massimiliano Masi[[23]](#footnote-23), titled "Capability Lookup, Service Location ABB, and Trust Model for the eHealth Domain", a mapping of services into SMPs is already described.

This mapping works quite well for the services, but is not obvious for the VPN and NCP gateway configuration, especially in the context of the used certificates. In the SML/SMP standard, certificates are attached to the service endpoint, and it is not quite clear, whether the endpoint certificates are used to proof the signature or if they are used for TLS communication. For the NPC definition the TSL provides two certificates, one for encryption and the other for signing. This differentiation of use of certificates in the SML/SMP definition is not foreseen. The definition of certificates in the service-endpoints might make the use of NPC signing certificates obsolete. In that case it would moves the responsibility form the NCP gateway to the service-endpoints. Anyway it is not clear whether endpoint-certificates needs to be defined or not, in case of a TSL-to-SML/SMP translation.

If we configure the VPN endpoint as a Service Supply Point, as it is done in TSL, we could only provide an IP address of the VPN endpoint and not an URI as it is foreseen in SML/SMP. IP addresses or Internet names are no URIs, because they require the definition of a schema, e.g. HTTP, FTP. For IPSec/VPN there is no such schema defined officially[[24]](#footnote-24). There are finally two options: Providing no valid URI by the use of only the IP address or Internet name, or define a non-official schema, e.g. URI=ipsec:176.65.73.16, which would be the more elegant way. The NPC gateway with its two certificates does not contain a service endpoint definition (at least in the version of the TSL file of Luxembourg that we had). The use of endpoint-URI is not obviously mandatory in the specification of SML/SMP, so it is assumed that this can be left out. But both NCP certificates must then be translated into two different services (e.g., "NCP-crypt", "NCP-sign") in the service metadata description.

With that, the information of the TSL file can somehow be translated into the service metadata description of the SML/SMP standard.

Questions have been addressed whether the distribution of certificates via SMPs are acceptable.

The trustworthiness of the given information depends in the SML/SMP case on the trustworthiness of the DNS server of the Internet-domain that is associated to the NCP.

1. It must be known somehow, what Internet domain an NCP is associated to.
2. The OASIS SMP/SML standards foresess the lookup in the DNS Meta:SMP record.
3. The validity of the given information in the record is ensured by the use of DNSSEC
4. The DNS Meta:SMP record is pointing to the SMP of the associated domain, where the service-metadata can be downloaded.
5. The service-metadata needs to be signed to ensure, that it is coming from the correct issuer.
6. The certificate that is being used for signing the service-metadata can be published in the DNS server in the TLSA-record via the DANE standard.
7. The validity of this also has to be ensured via DNSSEC.
8. With that, certificates of that are published in the service-meta are seen as being true.

It is not clear, whether the DNS server can be defined as secure node and how the administration of the DNS server is included into the audit trail. If the trust in the DNS server is not given, assumptions in the trust-chain of 1-8 also can be questioned.

Point 1 in the list is also not obvious. If a centralized server needs to be avoided, that creates the link between country and associated Internet domain, this link must be either implicit (=known rule to create the Internet domain of the NCP from the known country-code), or it must be configured in the system, once a country is added or the internet domain changes.

## Upload of Information to the SMP

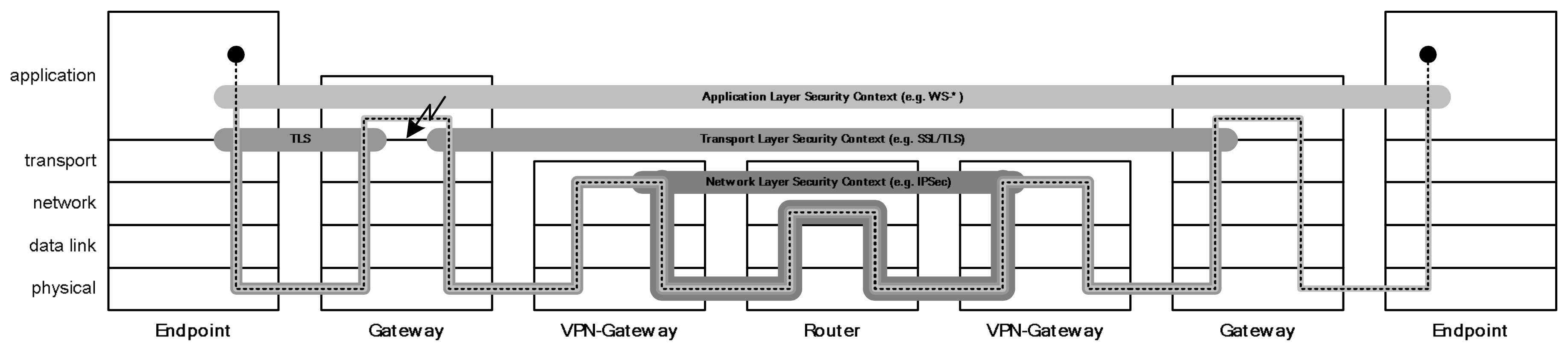
The provision of metadata information in the SMP can be performed in a similar way as it is currently done during the upload of information the central server. Alternatively the information could be stored in a configuration server first and all secure nodes including the SMP download their configuration periodically from there. An advantage of this would be the possibility that the SMP not only downloads the service metadata (service endpoints, certificates, etc.) that it wants to publish but also other relevant configuration parameter that it needs for the proper working of the server.

## Pros and Cons for the use of the SML/SMP standard

|  |  |
| --- | --- |
| Statement | Pro + Con - |
| Replacing the central server removes a single point of failure | + |
| TSL is a proprietary standard only valid in the epSOS context | + |
| SML/SMP standard can also be used for the definition of other/new services | + |
| Every country is responsible for the management publishing of its service descriptions | + |
| SML/SMP relies on the trustworthiness of the DNS server of a domain | - |
| DNS server is not defined as a Secure Node yet (audit trail?) | - |
| Implicit knowledge (creation rule) of the Internet domain of a new country | - |
| Trust relations are direct between to NCPs and not via an official National Trust Service Provider (TSP) | - |
| Migration to inherit direct trust by the use of National Trust Service Provider (TSP) is not discussed in the SML/SMP specifications. | - |

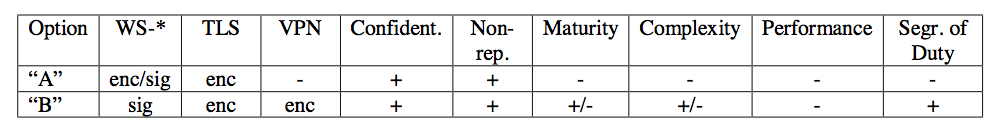
## End-to-End-Encryption and the use of VPN

In D.3.7.2. FINAL SECURITY SERVICES SPECIFICATION DEFINITION - Section II - Security Services[[25]](#footnote-25), it is explained, how end-to-end-security can be ensured in several layers. On the Network-Layer, e.g. via IPSec, on the Transport Layer, e.g., via TLS, and on the Application Layer e.g., vial WS-\*.



Security Realized on Different Layers of the OSI Reference Model

In the same document, a comparison between two different alternatives are discussed, one avoids the use of VPN connection (Option "A") and one that foresees the use of VPN connections (Option "B")



Comparison of pros/cons for (WS-\*enc/sig +TLS) vs (WS-\*sig +TLS+VPN)

The document concludes:

"*From the security point of view both options “A” and “B” guarantee an adequate level of protection.*"

In the current implementation, the use of VPN as protection of the network layer is used. It bases on IPSEC ESP in transport-mode. In contrast to IPSec in tunnel-mode, only the content of an IP packet is encrypted and not the header, so the IP header shows the destination of the communication and not of the gateway. This is not a security issue, if it is accepted that endpoint-IPs are public.

## Use of the TSL Information for VPN

For the setup of the VPN connection, the VPN gateway information in the TSL file is important.

After the uploading of the TLS file to the central service, other nations can download the file via the use of TLS-Synchronizer.

In case of a new country, the TLS-Synchronizer looks in its local database for which country it needs to download the TLS information (parameter "ncp.countries") and downloads the new TLS file then. This is also done in case of updated TLS files (including new certificates as part of the TLS file).

After downloading of the TLS file, the TSL-Synchronizer performs changes in the local database and adds new or changed certificates to the VPN server configuration. In case of OpenSwan this is done in the local keystore of the VPN server, in case of RedHat Enterprise, the certificates need to be imported into a special DB-file.

The key of the VPN server is stored in a separate keystore.

Certificates of the partner VPN must be known prior to the establishment of the VPN connection. As an example for each VPN connection OpenSwan needs a configuration file that makes a reference to the certificate:

# right is the host of their VPN server

right=195.20.133.178

# the certificate that they use for their VPN server

rightcert=vpn6.conet-services.de.der

# the ID of their VPN server - must be the same as in their conf

rightid=@vpn6.conet-services.de

# connection is not started on ipsec start, started by hand

auto=add

# perfect forward secrecy

pfs=yes

It is not possible to exchange the certificates during the setup of the connection, as it is done during HTTPS. Also we could not find VPN Servers that look for a certificate in the DNS server in the TLSA or IPSECKEY records that could be used to store pubic certificates or keys.

Ports on the VPN gateway identify the IPSec endpoints of the VPN tunnel. These ports can either be accessed by every machine in the Internet or are restricted by the existence of a firewall. Firewall rules that limit the access to only known machines require knowledge about the VPN gateways of the partner country. This information is given in the TSL file. To our knowledge, the TSL synchronizer does not automatically add or change the firewall rules on base of the given information. In fact the rules are set manually. There are firewalls that are scriptable regarding firewall rules. Consequences that derive out of this for audit trails cannot be estimated.

As an alternative, the firewall can be configured in a way that the access to the VPN ports of the VPN gateway is unrestricted. Since the firewall server only accepts connection requests from machines with known certificates, the setup of the VPN tunnel is not possible for unknown countries and therefore cannot only introduce a weakening for potential denial-of-service-attacks.

# Recommendations / Roadmap / Conclusions

1. The definition of Secure Node (SN) is inherited from the IHE ATNA specifications (www.ihe.net). A node is considered secure if the only mean to access Private Healthcare Information (PHI) is to use IHE-Secured transactions and if all the OS-level configuration changes are subject to Audit and Evidence. [↑](#footnote-ref-1)
2. D3.9.1 epSOS Pilot System Component Specification, version 1.0, 01/10/2010, http://www.epsos.eu/uploads/tx\_epsosfileshare/D3.9.1\_epSOS\_Pilot\_System\_Component\_Specification\_01.pdf [↑](#footnote-ref-2)
3. D3.A.7 epSOS Architecture and Design – EED Design - epSOS X.509 Certificate Profiles, version 1.0, 31/01/2014, http://eucases.eu/fileadmin/epSOS/documents/D3.A.7j\_epSOS\_EED-X.509-Profiles\_v1.0.pdf [↑](#footnote-ref-3)
4. Massimiliano Masi, Capability Lookup, Service Location ABB, and Trust Model for the eHealth Domain, 18/05/2015, https://openncp.atlassian.net/wiki/download/attachments/57671767/20150616\_Masi\_SMP-TRUST.docx?version=1&modificationDate=1434473128687&api=v2&download=true, https://openncp.atlassian.net/wiki/display/ncp/20150616+-+Meeting+minutes,+Tuesday,+June+16th,+2015+-+OpenNCP+-+SMP+(central+configuration)+-+Work+Progress+Meeting+1?preview=/57671767/57671792/20150616\_Masi\_SMP-TRUST.docx [↑](#footnote-ref-4)
5. ETSI: Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information. Version 3.1.2, December 2009.  
   http://www.etsi.org/deliver/etsi\_ts/102200\_102299/102231/03.01.02\_60/ts\_102231v030102p.pdf [↑](#footnote-ref-5)
6. D3.4.2 epSOS Common Components, version 1.00, 16/07/2010, http://www.epsos.eu/uploads/tx\_epsosfileshare/D3.4.2\_epSOS\_Common\_Components\_Specification\_01.pdf [↑](#footnote-ref-6)
7. D3.A.3 epSOS Architecture and Design – EED Design 2.0 – Interoperability Specification, version 1.0, January 2014, https://publicwiki-01.fraunhofer.de/epSOS\_specification/index.php/EpSOS\_D3.A.3\_Original\_Document [↑](#footnote-ref-7)
8. D3.A.7 epSOS Architecture and Design – EED Design – epSOS Messaging Profile, version 1.0, 31/01/2014, http://eucases.eu/fileadmin/epSOS/documents/D3.A.7g\_epSOS\_EED\_Messaging\_Binding-v1.0.pdf [↑](#footnote-ref-8)
9. S. Kent, K. Seo: Security Architecture for the Internet Protocol. December 2005 [↑](#footnote-ref-9)
10. T. Dierks, C. Allen: The TLS Protocol. Version 1.0. January 1999. [↑](#footnote-ref-10)
11. IHE International: IHE IT Infrastructure (ITI) Technical Framework. Volume 2a: Transactions. August 2009 [↑](#footnote-ref-11)
12. D3.7.2 Final Security Services Specification Definition (Master Document), version 0.4, 16/06/2010, http://www.epsos.eu/uploads/tx\_epsosfileshare/D3.7.2\_epSOS\_Final\_Security\_Services\_01.pdf [↑](#footnote-ref-12)
13. Ecrypt-II NoE: ECRYPT2 Yearly Report on Algorithms and Keysizes (2008-2009). July 2009. http://www.ecrypt.eu.org/documents/D.SPA.7.pdf [↑](#footnote-ref-13)
14. Bundesamt für Sicherheit in der Informationstechnik: BSI – Technische Richtlinie 03116 für die eCard-Projekte der Bundesregierung. Version 3.0. April 2009. [↑](#footnote-ref-14)
15. Secrétariat général de la défense nationale: Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse

    standard. Version 1.1. December 2006. [↑](#footnote-ref-15)
16. E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid (Eds.): NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General. March 2007. [↑](#footnote-ref-16)
17. Massimiliano Masi, Rainer Hörbe, NCP configuration files & epSOS central services specification, version 0.4, 04/07/2011 [↑](#footnote-ref-17)
18. https://www.dropbox.com/sh/ezyuq6vpxyiltfu/AACWnyonu5s0sxR3fUpMSzOva?dl=0 [↑](#footnote-ref-18)
19. Heise.de, Beliebige SSL-Zertifikate durch Missbrauch der Uralt-Internettechnik BGP, 10.8.2015 http://www.heise.de/newsticker/meldung/Beliebige-SSL-Zertifikate-durch-Missbrauch-der-Uralt-Internettechnik-BGP-2774454.html, Translation: "Any SSL Certificates through misuse of the age-old Internet technology BGP" https://translate.google.com/translate?sl=de&tl=en&js=y&prev=\_t&hl=de&ie=UTF-8&u=http%3A%2F%2Fwww.heise.de%2Fnewsticker%2Fmeldung%2FBeliebige-SSL-Zertifikate-durch-Missbrauch-der-Uralt-Internettechnik-BGP-2774454.html&edit-text=&act=url [↑](#footnote-ref-19)
20. epSOS Architecture and Design EED DESIGN – epSOS TSL Profile, version 1.0, 31.01.2014, http://eskills-guide.eu/fileadmin/epSOS/documents/D3.A.7i\_epSOS\_EED\_TSL\_Binding-v1.0.pdf [↑](#footnote-ref-20)
21. Fraunhofer Wiki: epSOS Trust Service List - ETSI TS 102 231 Binding, https://publicwiki-01.fraunhofer.de/epSOS\_specification/index.php/EpSOS\_Trust\_Service\_List\_-\_ETSI\_TS\_102\_231\_Binding [↑](#footnote-ref-21)
22. Fraunhofer Wiki: epSOS TSL Profile (TSL Synchronization), https://publicwiki-01.fraunhofer.de/epSOS\_specification/index.php/EpSOS\_TSL\_Profile\_(TSL\_Synchronization) [↑](#footnote-ref-22)
23. Massimiliano Massi: Capability Lookup, Service Location ABB, and Trust Model for the eHealth domain, 18. May 2015, https://openncp.atlassian.net/wiki/download/attachments/57671767/20150616\_Masi\_SMP-TRUST.docx?version=1&modificationDate=1434473128687&api=v2&download=true, https://openncp.atlassian.net/wiki/display/ncp/20150616+-+Meeting+minutes,+Tuesday,+June+16th,+2015+-+OpenNCP+-+SMP+(central+configuration)+-+Work+Progress+Meeting+1?preview=/57671767/57671792/20150616\_Masi\_SMP-TRUST.docx [↑](#footnote-ref-23)
24. IANA: Uniform Resource Identifier (URI) Schemes, http://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml [↑](#footnote-ref-24)
25. epSOS Delierable: Work Package Document - D.3.7.2. FINAL SECURITY SERVICES SPECIFICATION DEFINITION - Section II - Security Services, Version 0.4.21, 16/06/2010 [↑](#footnote-ref-25)