Capability Lookup, Service Location ABB, and Trust Model for the eHealth domain

*This document MUST be considered as a DRAFT. All the information contained are subject to discussion.*

*Massimiliano Masi –* *massi@tiani-spirit.com* *– 18 May 2015*

# Introduction

The epSOS project ended in June 2014. Its technical assets are under the intellectual property of the EXPAND project that will “hand over” both the specifications and the software (the OpenNCP) to the EU commission. Two additional EU LSPs are helping EXPAND in the process of maintaining and enhancing the epSOS legacies: e-SENS ([www.esens.eu](http://www.esens.eu)) and Trillium Bridge ([www.trilliumbridge.eu](http://www.trilliumbridge.eu)). In particular the e-SENS project eHealth pilot aims at exploiting the Building Blocks provided with a twofold goal: to align itself to the European Infrastructure of Cross-Border services, and to “fill the gaps” left open by the epSOS specifications.

In fact, at the moment of drawing up the epSOS specifications, several aspects have been “relaxed” in order to ease the start of the pilots. Notably, the following aspects have been tackled by e-SENS:

* *Lack of Non Repudiation protocol*. EpSOS only defined a set of audit trails to track the transactions
* *Central Configuration Services*. Being the epSOS National Contact Point for eHealth (NCPeH) a *Secure Node[[1]](#footnote-1)*, no manual configuration actions are allowed. Configuration items were fetched from a central configuration repository;
* *Trusted Service List*. Information about the remote’s certificates, endpoints, contact persons, were stored in a TSL, fetched regularly from the central configuration services;
* *Missing patient Electronic Identification*. EpSOS used a manual mean (e.g., based on member-state specific identity traits) to identify a patient, e.g., manual data-entry from the doctor’s office or pharmacy;
* *Relaxed Trust Bootstrap and Certificate profiles*. EpSOS’ trust bootstrap has been relaxed by using the mutually-acknowledged TSL. Also, at the moment of start piloting, few commercial CA[[2]](#footnote-2) was able to fulfill the epSOS certificate profile[[3]](#footnote-3).

## Navigating into the epSOS specifications

The epSOS security specifications are in the deliverable 3.7.2 “Security Services”, available from EXPAND or through the epSOS main website ([www.EpSOS.eu](http://www.EpSOS.eu)). In particular section 7.3 and 7.8 describe the need of having a Non-Repudiation protocol, and why it is relaxed. The epSOS Security Expert Group (SEG) deliverables define the certificate relaxations for the pilots. The definition of the TSL, the patient identification, and the Central Configuration Services, are profiled in the D3.4.2 “Common Components Specifications”. The content of the Central Configuration Services is however implementation specific. The deliverables D3.A.x[[4]](#footnote-4) links the sustainability of the epSOS requirements with the concepts of the ECCF enterprise architecture.

## Capability Lookup and Service Location

*The information here should be considered as proposal only, a discussion is expected*

The epSOS model is shown in the Figure 1. The NCPs fetch the configuration data from the Central Configuration services (e.g., using plain TCP or SCP) for the IHE transaction to be performed. Configuration data is cached indefinitely.



Figura 1 EpSOS Central Services

The eHealth domain may exploit the functionalities exposed by SMP and SL in order to overcome the underspecified central configuration services. Remote capabilities may contain the following

* Remote endpoint
* Remote trusted certificate
* Remote transport protocol (XCA or XCF)
* Which Identity Traits for the patient identification (e.g., fiscal code, SSN, name, surname, etc)
* Is eID supported?

And, going a bit further,

* Automatic configuration of clients (NCP-B) and servers (NCP-A)
* Terminology Services capabilities (e.g., RDF, OWL, FHIR)
* Security Assertion Broker (JWT to SAML)

At a first glance, the SMP mapping is performed by using one *ServiceGroup* for NCP. Each entry on the service group points to a specific epSOS service (e.g., patient service, order service). A sample mapping is shown below.

<?xml version="1.0" encoding="UTF-8"?>
<!-- This is the Service Group file for the German NCP, according with 4.5.8.1 epSOS EventIDs -->
<ServiceGroup xmlns="http://docs.oasis-open.org/bdxr/ns/SMP/2014/07"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://docs.oasis-open.org/bdxr/ns/SMP/2014/07 file:/Users/max/Downloads/bdx-smp-201407.xsd">
 <ParticipantIdentifier scheme="urn:epsos:2015:smp:scheme:participant\_id">urn:germany:ncpb</ParticipantIdentifier>
 <ServiceMetadataReferenceCollection>
 <!-- For the 1,2 transaction: should we group them, or we allow to have different endpoints for the same service? -->
 <!-- epsosIdentityService::FindIdentityByTraits epsos-docid-qns::urn:epsos:services##epsos-11 -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-11"/>
 <!-- epsosPatientService::List -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-21"/>
 <!-- epsosOrderService::List -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-31"/>
 <!-- epsosDispensationService::Initialize -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-41"/>
 <!-- epsosDispensationService::Discard -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-42"/>
 <!-- epsosConsentService::Put -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-51"/>
 <!-- epsosConsentService::Discard -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-52"/>
 <!-- identityProvider::HcpAuthentication -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-91"/>
 <!-- ncp::TrcAssertion -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-92"/>
 <!-- ncpConfigurationManager::ImportNSL -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-93"/>
 <!-- ncpTransformationMgr::Translate -->
 <ServiceMetadataReference href="http://smp.location.de/epsos-docid-qns%3A%3Aurn%3Aepsos%3Aservices%23%23epsos-94"/>
 </ServiceMetadataReferenceCollection>
</ServiceGroup>

In this example the Service Group is created for the German NCP. Each *MetadataReference* points to the document containing the *ServiceInformation*. A sample patient list is shown below.

<?xml version="1.0" encoding="UTF-8"?>
<SignedServiceMetadata xmlns="http://docs.oasis-open.org/bdxr/ns/SMP/2014/07"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://docs.oasis-open.org/bdxr/ns/SMP/2014/07 file:/Users/max/Downloads/bdx-smp-201407.xsd"
 xmlns:ns="urn:esens:smp">
 <ServiceMetadata>
 <ServiceInformation>
 <!-- Same as the service group -->
 <ParticipantIdentifier scheme="urn:epsos:2015:smp:scheme:participant\_id">urn:germany:ncpb</ParticipantIdentifier>
 <DocumentIdentifier scheme="epsos-docid-qns">epsos-docid-qns::urn:epsos:services##epsos-21</DocumentIdentifier>
 <ProcessList>
 <Process>
 <ProcessIdentifier scheme="urn:epsos:2015:smp:scheme:proc\_id">urn:germany:ncpb:epsosPatientService::List</ProcessIdentifier>
 <ServiceEndpointList>
 <Endpoint transportProfile="urn:ihe:iti:2013:xcpd">

 <EndpointURI>http://germany/ncp/patient/list</EndpointURI>
 <RequireBusinessLevelSignature>false</RequireBusinessLevelSignature>
 <MinimumAuthenticationLevel>urn:epSOS:loa:1</MinimumAuthenticationLevel>
 <ServiceActivationDate>2015-04-29T12:55:39Z</ServiceActivationDate>
 <ServiceExpirationDate>2015-04-29T12:55:39Z</ServiceExpirationDate>
 <Certificate>SGksIEkgYW0gYSBuaWNlIFg1MDkgQ2VydGlmaWNhdGU=</Certificate>
 <ServiceDescription>This is the epSOS Patient Service List for the German NCP</ServiceDescription>
 <TechnicalContactUrl>http://germany/contact</TechnicalContactUrl>
 <TechnicalInformationUrl>http://germany/contact</TechnicalInformationUrl>

 </Endpoint>
 </ServiceEndpointList>

 </Process>
 </ProcessList>

 </ServiceInformation>
 </ServiceMetadata>
 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
 <CanonicalizationMethod Algorithm=""></CanonicalizationMethod>
 <SignatureMethod Algorithm=""></SignatureMethod>
 <Reference>
 <DigestMethod Algorithm=""></DigestMethod>
 <DigestValue></DigestValue>
 </Reference>
 </SignedInfo>
 <SignatureValue></SignatureValue>
 </Signature>
</SignedServiceMetadata>

Similar Service Information are foreseen for the other NCP services. A particular note is to the SAML Identity Provider.

<?xml version="1.0" encoding="UTF-8"?>
<SignedServiceMetadata xmlns="http://docs.oasis-open.org/bdxr/ns/SMP/2014/07"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://docs.oasis-open.org/bdxr/ns/SMP/2014/07 file:/Users/max/Downloads/bdx-smp-201407.xsd"
 xmlns:ns="urn:esens:smp">
 <ServiceMetadata>
 <ServiceInformation>
 <!-- Same as the service group -->
 <ParticipantIdentifier scheme="urn:epsos:2015:smp:scheme:participant\_id">urn:germany:ncpb</ParticipantIdentifier>
 <DocumentIdentifier scheme="epsos-docid-qns">epsos-docid-qns::urn:epsos:services##epsos-91</DocumentIdentifier>
 <ProcessList>
 <Process>
 <ProcessIdentifier scheme="urn:epsos:2015:smp:scheme:proc\_id">urn:germany:ncpb:identityProvider::HcpAuthentication</ProcessIdentifier>
 <ServiceEndpointList>
 <Endpoint transportProfile="urn:ihe:iti:2013:xca">

 <EndpointURI>http://germany/ncp/idp/issue</EndpointURI>
 <RequireBusinessLevelSignature>false</RequireBusinessLevelSignature>
 <MinimumAuthenticationLevel>urn:epSOS:loa:1</MinimumAuthenticationLevel>
 <ServiceActivationDate>2015-04-29T12:55:39Z</ServiceActivationDate>
 <ServiceExpirationDate>2015-04-29T12:55:39Z</ServiceExpirationDate>
 <Certificate>SGksIEkgYW0gYSBuaWNlIFg1MDkgQ2VydGlmaWNhdGU=</Certificate>
 <ServiceDescription>This is the epSOS IdP for the German NCP</ServiceDescription>
 <TechnicalContactUrl>http://germany/contact</TechnicalContactUrl>
 <TechnicalInformationUrl>http://germany/contact</TechnicalInformationUrl>
 <Extension>
 <ns:IdpCertificate>GksIEkgYW0gYSBuaWNlIFg1MDkgQ2VydGlmaWNhdGU=</ns:IdpCertificate>
 <ns:SAMLIssuerURI>urn:tiani-spirit:sts</ns:SAMLIssuerURI>
 <ns:trustedSTS>
 <ns:sts>urn:austria:idp</ns:sts>
 <ns:sts>urn:italy:idp</ns:sts>
 <ns:sts>urn:france:idp</ns:sts>
 </ns:trustedSTS>
 </Extension>
 </Endpoint>
 </ServiceEndpointList>

 </Process>
 </ProcessList>

 </ServiceInformation>
 </ServiceMetadata>
 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
 <CanonicalizationMethod Algorithm=""></CanonicalizationMethod>
 <SignatureMethod Algorithm=""></SignatureMethod>
 <Reference>
 <DigestMethod Algorithm=""></DigestMethod>
 <DigestValue></DigestValue>
 </Reference>
 </SignedInfo>
 <SignatureValue></SignatureValue>
 </Signature>
</SignedServiceMetadata>

In fact, the Identity Provider needs additional information in order to operate, that is to build the trust relationships (i.e., a Federation) with the other NCPs.

*Questions:*

* *is this correct? Can certificates be exchanged using the SMP, in the NCP network?*
* *How to operate? Distributed or Centralized?*
* *Exchange of certificates: we believe that the certificates should be held in the Trust List. In fact the Trust list has a better supervision model and strong legal basis (ETSI and the Service Directive). TL are used more in the other domains to exchange certificates, rather than SMP (only used in PEPPOL, from e-SENS WP3). SMP should be used for all capabilities but not certificates.*

## Trust Establishment

The epSOS Trust Model is described in D3.7.2[[5]](#footnote-5). It inherits the IS27000 concept of *protection rings* and it is depicted in Figure 2.



Figura 2 EpSOS Security Zones

In particular, the epSOS Architecture is defined in section 4 (Overall Picture, Trust Relationships) and Section 5 (Data Exchange Security Service). The idea is to describe the security requirements of where PHI can be disclosed, what can be a data controller or a data processor. The semantics of the zones are here reported.

* 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).

The epSOS trust model follows the *direct brokered trust* paradigm. National Infrastructures have a direct trust with their NCPs, which trust themselves (as in section 4.3 of the e-SENS Trust Models whitepaper).

The epSOS SOA ecosystem is ready for the conclusion (Section 6) of the above mentioned e-SENS whitepaper with no conceptual changes.

1. The definition of Secure Node (SN) is inherited from the IHE ATNA specifications ([www.ihe.net](http://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. Some participating nations had to use ministry-level or national-level CA [↑](#footnote-ref-2)
3. The epSOS certificate profile was based on FIPS and NIST dictates. The problem was in the unavailability of hash functions greater than SHA-1 [↑](#footnote-ref-3)
4. Also available in the epSOS wiki: <https://publicwiki-01.fraunhofer.de/epSOS_specification/index.php/Main_Page> [↑](#footnote-ref-4)
5. Also available in the wiki: https://publicwiki-01.fraunhofer.de/epSOS\_specification/index.php/EpSOS\_Trust\_Zones [↑](#footnote-ref-5)