epSOS Change Proposal

Instructions

This is a template to propose changes to *epSOS Specifications*.

Once a *Final Text Change Proposal* is incorporated into the corresponding *epSOS Specification*, it is no longer maintained. Relevant CPs must be submitted against the updated epSOS Specification.

The CP publication process is described in detail at www.xxxx.org

In submitting a new Change Proposal, the submitter should assign the MS Word file an initial filename including the submitters initials, and a few words describing the topic, eg: CP-epSOS-eHealth-<author initials>-<3/4 wordSummary>.docx>. The the expert Committee will assign a name (using the convention described below) when it is accepted for processing.

CPs should be submitted to the the epSOS expert Committee by e-mail at: e-mail@xxx.com

Please complete the following fields in the Change Proposal Summary Information: (a) Title, (b) epSOS Specification(s) affected, (c) submitter name and e-mail address and (d) provide detailed Rationale for Change and Proposed Change. Please fill in the Impact of Change and other fields if known.

**Red text is explanatory. Please delete this preamble and replace the red text below with appropriate responses in black text.**

Tracking information:

|  |  |
| --- | --- |
| EpSOS Specifciation (IS-nnnn or UC-pppp and title) | D3.4.2 |
| Change Proposal ID: | CP-<EpSOS >-<number>-<version>.doc (assigned by the EpSOS expert Committee) |
| Change Proposal Status: | Submitted |
| Date of last update: | 29/6/2015 |
| Person assigned: | (assigned by EpSOS expert Committee) |

Change Proposal Summary information:

|  |
| --- |
| Add the e-SENS Evidence Emitter ABB/SBB |
| Submitter’s Name(s) and e-mail address(es): | Massimiliano.masi@tiani-spirit.com |
| Submission Date: | 29/6/2015 |
| Specification numbers (IS-xxxx) affected: | D3.4.2 / D3\_A\_3 |
| Use Case Actor(s) and/or Requirement Number affected: | epSOS Trusted Service List |
| Section(s) affected: | 4.4 |
| Rationale for Change:The epSOS specifications tackle the problem of the configuration of remote NCPs by means of ad hoc Trust Service Status Lists, named NCP Service Status List (NSL). By exchanging NSL files amongst NCP installations, the capabilities of the remote country's installation are listed in this signed file. EpSOS NCPs shall follow the ATNA Secure Node definition. In fact, being the NCP installation a data processor, Private Healthcare Information (PHI) may risk to be disclosed e.g., by a misconfiguration of the system, or by a phisical access to the machine. For instance, section 6.7 of D3.7.2 states "the MACHINE(s) hosting the audit collection processes and the audit data (logs) must be UNACCESIBLE by Technical Staff users; users allowed/entitles to access the audit system will ONLY have the right to access in READING the logs, without having access to other system functions".These functionalities are achieved using non-standard solutions such the already mentioned NSL and the piloting solution named "syncapp". These two solutions exploited Central Configuration Services (CCS), a set of apache-and ssh-based services providing document store and retrieve functionalities. CCS were structured in two areas: a public area, and a private area. Public area contained information about routing, public certificates, endpoints, working hours, etc. While private area contained information about the configuration of the NCP (such as access control policies, trust relationships, etc). The OASIS-OPEN Business Document Exchange Service Metadata Publishing, BDX-SMP, offers a standard mean to achieve the abovementioned goals. In particular, SMP+SML offers a potential distributed approach to discover remote's NCP capabilities and local private configuration information by using a set of REST-based calls. Although a centralized SMP approach may fulfill the epSOS requirements, the experience of the SMP architects contacted suggests to architect a SMP+SML scenario. This is to prepare the NCP implementation to run in a distributed setting without any change on the client implementation. It has been decided to rename most of the epSOS URLs to a new structure. |

Formulate the proposed change here, if known at time of submission

Specify what exactly should be changed. When modifying existing text, paste it into this Change Proposal and DO NOT use MS Word change tracking. Manually format all changed text to **bold** and either **underline the new text** or **~~cross out the text to be removed~~**.

When pasting from documents use “Paste Special…”, select “Unformatted text”, and apply the appropriate styles to the text inserted. This avoids importing spurious paragraph formats (which are the cause of significant headaches for editors).

Proposed changes should be introduced with “editors instructions” in a “box” such as:

Replace Section X.X by the following:

or

Replace Section 4.4 of WP3.A\_EEDD\_II with the following:

## SMP

Network addresses, web service endpoints and certificates of a country's epSOS service providers and consumers are registered in a SMP SignedServiceMetadata structure, digitally signed by a trusted authority of the respective country (see [epSOS D3.7.2] for details). SignedServiceMetadata of all member states are obtained by a NCP using the SMP+SML protocol set and it will be cached by the NCPs (caching strategies are not tackled by this specifications).

SignedServiceMetadata are pointed by a overarching data structure, named ServiceMetadataCollection, that holds all the services exposed by a NCP. Figure XX and XY shows the structure



Figure 1 ServiceMetadataCollection data structure



Figure 2 SignedServiceMetadata

 The following sections define the application of the BDX-SMP for encoding the NCP configuration entries.

### ServiceMetadataCollection

*The ServiceMetadataCollection is a file containing all the pointers for the SignedServiceMetadata, configuration repositories for the NCP's capabilities.* Each entry on the service group points to a specific epSOS service (e.g., patient service, order service).

The fields for the ServiceGroup MUST be used as folloes for encoding the epSOS services.

|  |  |  |
| --- | --- | --- |
| **ServiceGroup Element** | **Opt** | **Usage Convention** |
| ParticipantIdentifier | R | MUST be the unique uri of the NCP (e.g., urn:germany:ncpeh) |
|  | ServiceMetadataReferenceCollection | R | Holds the pointers to the service |
|  | ServiceMetadataReference | O | If present, it MUST contain the URL of the SignedServiceMetadata file associated for the service. The format of the URL is http://<server location>/ehealth-resid-qns/<service\_url> |

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 SignedServiceMetadata.

### SignedInformation

The SignedInformation file contains the information realted to the specific eHealth resource (e.g., epSOS service). The following encoding MUST apply.

|  |  |  |
| --- | --- | --- |
| **SignedServiceMetadata** | **Opt** | **Usage Convention** |
| ParticipantIdentifier | R | MUST be the unique uri of the NCP (e.g., urn:germany:ncpeh) |
|  | DocumentIdentifier | R | it MUST contain the URL of the this SignedServiceMetadata file associated for the service. The format of the URL is http://<server location>/ehealth-resid-qns/<service\_url> |
|  | DocumentIdentifier/@Scheme | R | It MUST be ehealth-resid-qns |
|  | ProcessList | R | It holds the processes that provide services for the specific service |

Each process is encoded as follows.

|  |  |  |
| --- | --- | --- |
| **Process** | **Opt** | **Usage Convention** |
| ProcessIdentifier | R | MUST contain the URI of the specific service |
| ProcessIdentifier/@Scheme | R | MUST be urn:ehealth:smp:scheme:proc\_id |
| ServiceEndpointList | R | MUST contain the service information for each service endpoint served by this service. E.g., if service is Patient Service, the operation is List(). |
|  | Endpoint/@transportProfile | R | MUST contain the selected profile for this service. Available profiles are: * urn:ihe:iti:2013:xcpd
* urn:ihe:iti:2013:xds
* urn:ihe:iti:2013:xca
* urn:ihe:iti:2013:xcf

Applications MAY add additional protocols (e.g., for eID) |
|  |  | EndpointURI | R | MUST contain the WSE of the specific service |
|  |  | RequireBusinessLevelSignature | R | MUST be set to False (as it is not used by eHealth) |
|  |  | MinimumAuthenticationLevel | O | MAY contain the minimum Level of Authentication (LoA, AAL) required to access to the service.  |
|  |  | ServiceActivationDate | R | MUST contains the Date when the service has started |
|  |  | ServiceExpirationDate | O | MUST contains the Date when the service will be stopped |
|  |  | Certificate | R | MUST contain the public certificate used to run the service |
|  |  | ServiceDescription | O | MAY contain the english description of the service |
|  |  | TechnicalContactURL | O | MAY contain the information related to the technical contact |
|  |  | TechnicalInformationURL | O | MAY contain the URL pointer to the remote service technical description |
|  | Extension | O | MAY contain additional service-specific extension (processcontent = LAX) |

A sample SignedInformation file for the patient service 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>

Every SignedServiceMetadata MUST be signed by its scheme operator. The XML signature MUST be applied by using the *ServiceMetadata/ds:Signature* element as defined below

|  |  |
| --- | --- |
| **Signature Parameter** | **Usage Convention** |
| CanonicalizationMethod | SHOULD be "http://www.w3.org/2001/10/xml-exc-c14n#" |
| Transformation | Exclusive XML canonicalization SHOULD be used ([http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n), acc. [W3C XMLDSig] and [W3C XML-EXC 1.0]). As inclusive namespaces other prefixes than the ones defined in section **Error! Reference source not found.** of this document MUST NOT be used. |
| SignatureMethod | The signature method MUST comply with the epSOS recommendations on algorithms and key lengths (see section ...). For signing epSOS NSL the signature method "http://www.w3.org/2000/09/xmldsig#rsa-sha1" SHOULD be used. |
| DigestMethod | The hash algorithm MUST comply with the epSOS recommendations on algorithms and key lengths (see section ....). For signing epSOS NSL the digest method "http://www.w3.org/2000/09/xmldsig#sha1" SHOULD be used. |
| KeyInfo | This element MUST contain a ds:X509Data element which contains the X.509 certificate of the NSL scheme operator. |

### NCP Provider Identification

The ServiceMetadataReferenceCollection element MUST contain a single ServiceMetadataReference element for each face of the NCP (NCP-A and/or NCP-B) that is operated by the respective member state.

The service list for each face of the NCP contains entries for the gateways and services of this NCP. The following table shows, which service entries are mandatory (M) or optional (O) for service providers (NCP-A) and service consumers (NCP-B).

|  |  |  |  |
| --- | --- | --- | --- |
| **Gateway / Service** | **Opt. NCP-A** | **Opt. NCP-B** | **Reference** |
| VPN Gateway | R | R |  |
| NCP | R | R |  |
| Patient Identification Service | R | X |  |
| Patient Service | O | X |  |
| Order Service | O | X |  |
| Dispensation Service | O | X |  |
| Consent Service | O | X |  |
| HCP Identity Provider | X | O |  |
| HCP Signature CA | O | O |  |

### VPN Gateway Status Information

VPN Gateways status information entries are used to announce the address and digital ceritficate of a NCP’s VPN gateway.

|  |  |  |
| --- | --- | --- |
| **Process** | **Opt** | **Usage Convention** |
| ProcessIdentifier | R | MUST contain "urn:ehealth:ncp:vpngateway" |
| ProcessIdentifier/@Scheme | R | MUST be urn:ehealth:smp:scheme:proc\_id |
| ServiceEndpointList | R | If multiple gateway addresses are given, NCP-B MAY select among these. |
|  | Endpoint/@transportProfile | R | ?? Can we use this for setting up the VPN?? Can we write here if we have OpenSWAN, Cisco, etc? |
|  |  | EndpointURI | R | Fully qualified domain names and/or IP-addresses of the VPN gateway. This field is required for NCP-A and MUST not be used for NCP-B |
|  |  | RequireBusinessLevelSignature | X |  |
|  |  | ServiceActivationDate | R | MUST contains the Date when the service has started |
|  |  | ServiceExpirationDate | R | MUST contains the Date when the service will be stopped |
|  |  | Certificate | R | VPN gateway certificate (base64 encoded). Multiple gateway certificates MAY be provided. Each of these MUST comply with the epSOS VPN gateway certificate profile as defined in section ... of this document. |
|  |  | ServiceDescription | O | MAY contain the english description of the service |
|  |  | TechnicalContactURL | O | MAY contain the information related to the technical contact |
|  |  | TechnicalInformationURL | O | MAY contain the URL pointer to the remote service technical description |
|  | Extension | O | MAY contain additional service-specific extension (processcontent = LAX) |

### Use of Dedicated epSOS Identity Providers

Country-B implementations MAY use dedicated Identity Providers within NCP-B for issuing HCP Identity Assertions. In this scenario the HCP Identity Assertion MUST be signed by the Identity Provider. Identity Provider status information can be used for distributing the Identity Provider certificate.

|  |  |  |
| --- | --- | --- |
| **Process** | **Opt** | **Usage Convention** |
| ProcessIdentifier | R | MUST contain "urn:ehealth:ncp:<country>:ncpb-idp" |
| ProcessIdentifier/@Scheme | R | MUST be urn:ehealth:smp:scheme:proc\_id |
| ServiceEndpointList | R |  |
|  | Endpoint/@transportProfile | R | The transport profile used to validate an assertion. It MAY be one of* WS-Trust 1.3
* SAML Protocol v2
* OAuth 2.0

No furthere profiling here. It may be interesting for NCP-A to validate the assertion received. |
|  |  | EndpointURI | R | Fully qualified domain names and/or IP-addresses of the dedicated IDP |
|  |  | RequireBusinessLevelSignature | X |  |
|  |  | ServiceActivationDate | R | MUST contains the Date when the service has started |
|  |  | ServiceExpirationDate | R | MUST contains the Date when the service will be stopped |
|  |  | Certificate | R | Certificate that this IDP is using to sign |
|  |  | ServiceDescription | O | MAY contain the english description of the service |
|  |  | TechnicalContactURL | O | MAY contain the information related to the technical contact |
|  |  | TechnicalInformationURL | O | MAY contain the URL pointer to the remote service technical description |
|  | Extension | O | MAY contain additional service-specific extension (processcontent = LAX) For instance, the list of trusted remote IdPs.  |

### International Search Mask

EHealth portals use an adaptive Internation Search Mask configuration to switch the presentation of the portal for the specific patient's country.

|  |  |  |
| --- | --- | --- |
| **Process** | **Opt** | **Usage Convention** |
| ProcessIdentifier | R | MUST contain "urn:ehealth:ncp:<country>:ism" |
| ProcessIdentifier/@Scheme | R | MUST be urn:ehealth:smp:scheme:proc\_id |
| ServiceEndpointList | R |  |
|  | Endpoint/@transportProfile | R | MUST be "urn:ehealth:transport:none" |
|  |  | EndpointURI | X |  |
|  |  | RequireBusinessLevelSignature | X |  |
|  |  | ServiceActivationDate | R | MUST contains the Date when the mask has been issued |
|  |  | ServiceExpirationDate | O | MUST contains the Date when the service will be stopped |
|  |  | Certificate | X |  |
|  |  | ServiceDescription | O | MAY contain the english description of the search mask |
|  |  | TechnicalContactURL | O | MAY contain the information related to the technical contact |
|  |  | TechnicalInformationURL | O | MAY contain the URL pointer to the remote mask technical description |
|  | Extension | R | MUST contain the international search mask XML as direct children |

# Open Issues

* These requirements are for public information only. There is no classification of data. Removing of NSL has been indicated by the OpenNCP community as top priority for the e-SENS. As a future work, the access to classified information is a wish. But this will require to have forms of confidentiality, such as authN and authZ. These are in the roadmap of SMP.
* Exploit the usage of SMP for automatic VPN configuration is very important, but postponed for now
* FutureID Authentication Plans. In order to have eID level 2, some additional information shall be located by the LAM/LARMS/DCA components (e.g., where the TRC-STS is located? Which certificate should I use to connect?)
* How to use URL location? PEPPOL suggests the following
                http://<hash over recipientID>.<schemeID>.<SMLdomain>/<recipientID>/services/<documentType
This can help us constructing as follows: I want to obtain the configuration of the NCP-B STS of a remote country, thus I do hash("SAML NameID of the remote's issuer") concatenated to the schemeID ("urn:ehealth:smp:scheme:proc\_id ") in the SML Domain (tbd) concatenated with the recipient ID (SAML NameID of the remote's issuer) and the documenttype urn:ehealth:ncp:<country>:ncpb-idp. By constructing this URL, the SML returns the pointer to the SMP which holds the SignedInformation
* How to invalidate the cache? Errors related to the SMP information are easily catchable (e.g., SSLHandshakeException) and thus the cache invalidated.

# Mapping from TSL

The following mapping will apply. This is the mapping from an Envelope, which does not exist in SMP. If such records are considered, they SHOULD be part of the ServiceGroup.

|  |  |
| --- | --- |
| @TSLTag | n/a |
| @ID | n/a |
| SchemeInformation | n/a |
| TSLVersionIdentifier | n/a |
| TSLSequenceNumber | n/a |
| TSLType | n/a |
| SchemeOperatorName, SchemeOperatorAddress | Technical Contact and technical contact url, for each service |
| SchemeName | n/a |
| SchemeInformationURI | n/a |
| StatusDeterminationApproach | n/a |
| SchemeTypeCommunityRules | n/a |
| SchemeTerritory | n/a |
| PolicyOrLegalNotice | n/a |
| HistoricalInformationPeriod | n/a |
| PointersToOtherTSL | n/a |
| ListIssueDateAndTime | n/a |
| NextUpdate | n/a (SMP is cached) |
| DistributionPoints | n/a |
| SchemeExtensions | n/a |
| Signature | Mapped in the ServiceGroup signature |

### VPN Gateway Status Information

|  |  |
| --- | --- |
| ServiceTypeIdentifier | ProcessIdentifier *note that the new urn is just a suggestion. the old URL can still be used* |
| ServiceName | n/a |
| ServiceDigitalIdentity | Certificate |
| ServiceStatus | n/a *note that this is important. The service expiration time can be used to change the status, or in the extension* |
| StatusStartingTime | ServiceActivationDate |
| SchemeServiceDefinitionURI | n/a |
| ServiceSupplyPoints | Endpoint URI |
| TSPServiceDefinitionURI | n/a |
| ServiceInformationExtension | n/a |
| ServiceHistory | n/a |

### epSOS NCP Status Information

|  |  |
| --- | --- |
| ServiceInformation | n/a |
| ServiceName | n/a *is it needed?* |
| ServiceDigitalIdentity/X509Certificate | Certificate *One certificate per instance? Two certificates?* |
| ServiceStatus | n/a. *In fact, to use either we use the extension, or we remove it. The spec says: "After epSOS pilot phase 1 NCPs MUST NOT connect to other NCPs with a status other than "in accordance".* |
| StatusStartingTime | ServiceActivationDate |
|  |  |
|  |  |

The epSOS Service Status information is encoded as per Section 1.1.2.