|  |  |
| --- | --- |
| logo_ec_17_colors_300dpi | EUROPEAN COMMISSION  DIGIT  Connecting Europe Facility |

Service Metadata Publishing (SMP) Version 0.04

eHealth Project's Specificities

Document Approver(s):

|  |  |
| --- | --- |
| **Approver Name** | **Role** |
| Adrien FERIAL | Architect |
|  |  |
|  |  |

Document Reviewers:

|  |  |
| --- | --- |
| **Reviewer Name** | **Role** |
| Adrien FERIAL | Architect |
|  |  |
|  |  |

Summary of Changes:

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Created by** | **Short Description of Changes** |
| 0.01 | 24/06/2016 | Yves ADAM | Creation – extract form ICD v0.15 |
| 0.02 | 11/07/2016 | Yves ADAM | Integrate comments of João Cunha and Massimiliano Masi |
| 0.03 | 12/07/2016 | Yves ADAM | Integrate comments of João Cunha |
| 0.04 | 25/07/2016 | Yves ADAM | Move additional signature from "ServiceInformation/Extension" to "Endpoint/Extension" |

Table of Contents

[1. Introduction 4](#_Toc457223511)

[1.1. OASIS/EHealth equivalence 4](#_Toc457223512)

[1.2. eHealth SMP administration process with a single centralized SMP 5](#_Toc457223513)

[1.3. eHealth signature of ServiceMetaData 6](#_Toc457223514)

[1.3.1. Signature of UC04 - Create or Update Service Metadata 6](#_Toc457223515)

[1.3.2. Signature of UC07 - Retrieve Service Metadata 7](#_Toc457223516)

[2. Document source files 9](#_Toc457223517)

Introduction

This document is an extension to the Interface Control Document of eDelivery SMP.

Is discusses major specificities related to eHealth project and is therefore not to be considered as reference for other implementations.

OASIS/EHealth equivalence

The following table introduces major SMP terms and link them to eHealth equivalents.

| **SMP** | **Definition and references to eHealth** |
| --- | --- |
| Access Point (AP) | NCP |
| ServiceMetadata | Data structure registered in a SMP holding Network addresses, web service endpoints and certificates of a country's epSOS service providers and consumers |
| ServiceMetadataCollection | Data structure are registered in a SMP holding all the services exposed by a NCP |
| ServiceMetadataReference | URL of the ServiceMetadata file associated for the service. The scheme of the URL is  /{identifier scheme}::{id}/services/{docType}  which expands to  /{identifier scheme}::{id}/services/{document identifier scheme}::{document identifier}  Example:  http://smp.location.de/ehealth-participantid-qns%3A%3Aurn%3Aehealth%3Ade%3Ancpb-idp/services/ehealth-resid-qns%3A%3Aurn%3A%3Aepsos%3Aservices%23%23epsos-11 |
| ParticipantIdentifier | unique uri of the NCP (e.g., urn:germany:ncpeh) |
| DocumentIdentifier/@Scheme | "ehealth-resid-qns" |
| ProcessIdentifier | URI of the specific service |
| ProcessIdentifier/@Scheme | "ehealth-procid-qns" |
| ServiceEndpointList | Service information for each service endpoint served by this service. E.g., if service is Patient Service, the operation is List(). |
| Endpoint/@transportProfile | Profile for this service. E.g.:  • urn:ihe:iti:2013:xcpd • urn:ihe:iti:2013:xds • urn:ihe:iti:2013:xca • urn:ihe:iti:2013:xcf |
| EndpointURI | WSE of a specific service |
| RequireBusinessLevelSignature | not used by eHealth |
| TechnicalContactURL | Information related to the technical contact |
| TechnicalInformationURL | URL pointer to the remote service technical description |

eHealth SMP administration process with a single centralized SMP

In the SMP administration model required by eHealth, only one SMP manages all ServiceGroups. That single SMP instance could be either hosted by DIGIT or the responsible authority of the business. eHealth will host its SMP instance.

The central authority owns the two users “System Admin” and “Admin SMP”.

This process is a simplified version of the distributed one. In that case:

* There may be only one "Admin ServiceGroup" (still multiple may also be defined as above).
* Since "Admin ServiceGroup" users are in a secure environment, basic authentication could be used instead of a certificate with 2-way-ssl.

In step of the picture besides, "*Admin ServiceGroup A, B, C, D, E, F*" defines some of the services for one or several parties among all.

eHealth signature of ServiceMetaData

This section describes how ServiceMetadata are signed in the context of eHealth domain. This relates to use cases (and services) UC04 – "Create or Update Servivce Metadata" and UC07 - "Retrieve Service Metadata".

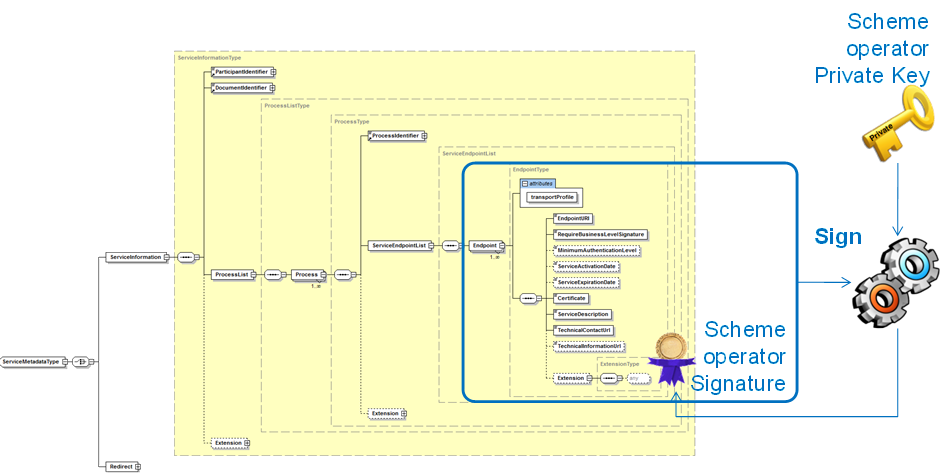
The objectives are:

* to allow the SMP to verify that the registration of ServiceMetadata is requested by the correct scheme operator;
* to allow the NCP (acting as a sender) to verify that the ServiceMetadata provided by the SMP were provided to the SMP by the correct NCP, thus, signed by a scheme operator in the country’s national infrastructure.

This solution will make use of the free extension section of the XML that is available in the standard OASIS and ETSI XaDES formats with no change. This solution is consequently fully in-line with the existing specifications.

Signature of UC04 - Create or Update Service Metadata

* At registration time the scheme operator of the country of the receiving NCP signs **all** the *Endpoint* data using the scheme operator's certificate, and then adds the resulting signature into the all the Extension (of the service Endpoints list):

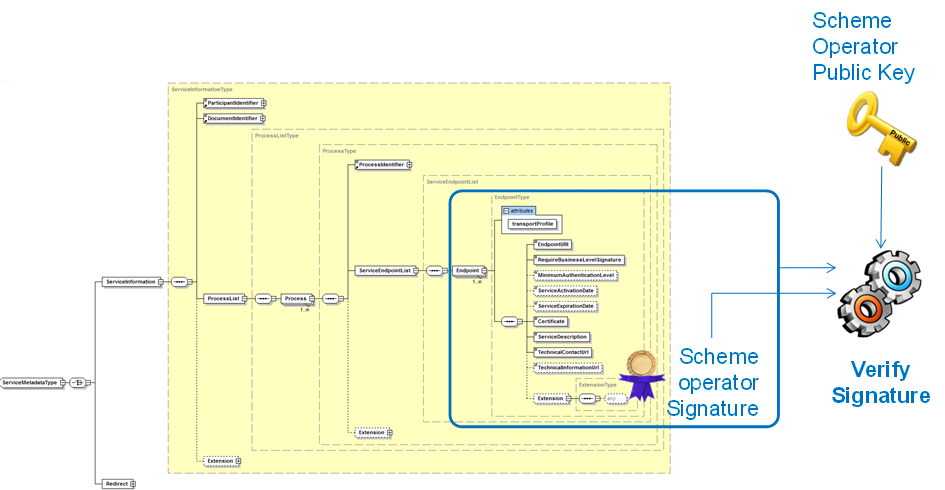


* When it receives the registration request, the SMP verifies that the all the *Endpoint* 's have been signed with the Certificate of the correct scheme operator. In that purpose it simply removes the signature from the Endpoint/Extension and then validates the file (without this element) against that signature with the public key of the scheme operator of the country of the receiving NCP:

Signature of UC07 - Retrieve Service Metadata

* When resolving the recipient's capabilities, the NCP (acting as Sender) uses the SignedServiceMetadataType in the standard way to sign the SeviceMetadata (as defined in [REF5] – §2.3.5 and Appendix C).  
  
* upon reception of the requested ServiceMetadata, the NCP (acting as sender) will verify both signatures:
  + the NCP verifies the signature of the SMP which is part of the ServiceMetadata, as in the standard way (cf. [REF5] – §2.3.5 and Appendix C) :



* + the NCP verifies that the *Endpoint* 's data have all been signed by the scheme operator using its certificate (like the SMP does upon registration of the ServiceMetadata):

**! Important remark**: it is the responsibility of the scheme operator (of the receiver) to ensure that the signature of the Endpoint's data are valid in the SMP at any time; i.e. to update its Metadata (i.e. the "*Endpoint*" data in particular) with the signature of its new certificate before its old certificate is revoked to allow the NCP to verify the signatures of these *Endpoint*'s data.

Document source files

The attached files contain table and drawings included upper in this document and are included to facilitate future updates of this document.



TODO (for each release): replace updated Excel and Powerpoint files.