



EUROPEAN COMMISSION

DIGIT
Digital Europe Programme

Service Metadata Provider

Interface Control Document

DomiSMP 5.0

Version [2.1]

Status [Final]

© European Union, 2023

Reuse of this document is authorised provided the source is acknowledged. The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents.

Date: 23/06/2023

Document Approver(s):

Approver Name	Role
Bogdan DUMITRIU	Project Manager

Document Reviewers:

Reviewer Name	Role
Joze Rihtarsic	Developer
Caroline AEBY	TESO Support

Summary of Changes:

Version	Date	Created by	Short Description of Changes
0.1	12/01/2016	Yves ADAM	Initial version
0.2	22/01/2016	Yves ADAM	Additions and corrections based on discussion with Adrien Ferial
0.3	26/01/2016	Yves ADAM	Additions and corrections based on SMP/SML task force meeting
0.4	28/01/2016	Yves ADAM	Additions and corrections based on discussion with Adrien Ferial
0.5	29/01/2016	Yves ADAM	Additions and corrections based on discussion with Adrien Ferial
0.6	04/02/2016	Yves ADAM	Additions and corrections based on feedback from João Cunha
0.7	17/02/2016	Yves ADAM	More additions and corrections based on feedback from João Cunha
0.8	23/02/2016	Yves ADAM	Update deriving from task force discussions of Feb 17th
0.9	29/02/2016	Yves ADAM	Corrections based on discussion with Adrien Ferial
0.10	24/03/2016	Yves ADAM	Corrections based on feedback from João Cunha and discussions with Adrien Ferial
0.11	20/04/2016	Yves ADAM	Corrections based on feedback from João RODRIGUES FRADE
0.12	26/04/2016	Yves ADAM	More additions and corrections based on feedback from João Cunha
0.13	17/05/2016	Yves ADAM	Minor correction after conference call of April 29 th
0.14	26/05/2016	Yves ADAM	Fix corrupted image
0.15	24/06/2016	Yves ADAM	Specify specific signature solution of metadata for eHealth
0.16	24/06/2016	Yves ADAM	Extract eHealth specificities to another document
0.17	15/11/2016	Yves ADAM	Apply changes to error management, new

			namespace, new OASIS XSD
0.18	23/12/2016	Yves ADAM	Apply changes to use OASIS XSD as input for admin services
0.19	11/01/2017	Yves ADAM	Corrections based on feedback from João Cunha
0.20	20/01/2017	Yves ADAM	Apply standard template
0.21	07/02/2017	Yves ADAM	Corrections based on feedback from João Cunha
1.00	07/02/2017	Yves ADAM	Validated version
1.01	16/06/2017	Yves ADAM	Correction for release 3.0.0
1.02	28/06/2017	Yves ADAM	Correction for release 3.0.0
1.03	24/01/2018	Yves ADAM	Correction for release 4.0.0
1.04	20/03/2018	CEF Support	Reuse notice added
1.05	01/10/2018	Caroline AEBY	No more standby service
1.06	03/05/2022	Caroline AEBY	No more CEF references + links update
1.07	19/05/2022	Caroline AEBY	Email eDelivery support changed to EC-EDELIVERY
2.0	02/05/2023	Jože RIHTARŠIČ	Apply changes for release 5.0 RC
2.1	22/06/2023	Caroline AEBY	Domibus 5.0 FR

Table of Contents

1. INTRODUCTION.....	6
1.1. Background	6
1.2. Purpose of the Interface Control Document	6
1.3. Scope of the document.....	6
1.4. Audience	6
1.5. Definitions.....	6
1.6. References	7
2. INTERFACE DEFINITION	9
2.1. Positioning SMP in eDelivery	9
2.1.1. eDelivery in a nutshell.....	9
2.1.2. SMP role.....	10
2.1.3. SMP / SML interactions.....	10
2.2. Data model.....	12
2.2.1. Logical data model	12
2.2.2. XSD files.....	17
2.3. Use cases summary.....	18
2.3.1. Actors	18
2.3.2. Use cases diagram.....	19
2.3.3. Use case list.....	20
2.3.4. Story	22
2.4. Administration use cases	23
2.4.1. UC01 - Manage Administrators.....	23
2.4.2. UC02 - Create or Update Service Group	25
2.4.3. UC03 - Erase Service Group	31
2.4.4. UC04 - Create or Update Service Metadata	35
2.4.5. UC05 - Erase Service Metadata.....	43
2.5. Information retrieval use cases	46
2.5.1. UC06 - Retrieve Service Group.....	46
2.5.2. UC07 - Retrieve Service Metadata	50
2.6. Security	57
2.6.1. User management.....	57
2.6.2. Access rights.....	61
2.6.3. HTTP Authentication	61
2.6.4. Reverse proxy.....	62
2.6.5. Auditing.....	64
2.7. Special requirements	66
3. ANNEX	67
3.1. XSD files.....	67
3.1.1. Original official OASIS SMP XSD	67

3.1.2. Extended SMP XSD..... 71

3.2. Errors codes table 71

3.3. Detailed Errors structure 74

4. LIST OF FIGURES 75

5. LIST OF TABLES..... 75

6. CONTACT INFORMATION..... 76

1. INTRODUCTION

1.1. Background

The eDelivery building block helps public administrations exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way. By using this building block, every participant becomes a node in the network using standard transport protocols and security policies. eDelivery is based on a distributed model, allowing direct communication between participants without the need to set up bilateral channels.

1.2. Purpose of the Interface Control Document

This document will univocally define the participant's interface to the SMP component of the eDelivery building block as it will extend and evolve in sight of its usage in the framework of eHealth and its additional requirements.

This use case / interface control document will be used as reference for mutual understanding of eHealth requirements on the one hand and the future service delivered by the Digital Europe Programme on the other hand.

1.3. Scope of the document

This document is a high-level functional definition of the services provided by the SMP. This document will be later extended with additional document that further detail the services with technical information intended for the development of eHealth client solutions implementation.

1.4. Audience

This document is intended to:

- The architect and development teams of the Digital Europe Programme for committing on future service delivery of SMP
- The architects and functional analysts of the eHealth team for validating the intended service against their requirements.

1.5. Definitions

All the concepts used throughout this document have been defined in the following documents:

- [\[REF3\]](#)
- [\[REF4\]](#)
- [\[REF7\]](#)

1.6. References

#	Document	Contents outline
[REF1]	What is eDelivery?	Overview of eDelivery
[REF2]	Using HTTP Methods for RESTful Services	Short description of HTTP Methods for RESTful Services
[REF3]	<i>OpenPEPPOL AISBL - Policy for use of Identifiers</i>	
[REF4]	<i>OASIS - Service Metadata Publishing (SMP) Version 1.0 - Committee Specification 01</i>	This document describes a protocol for publishing service metadata within a 4-corner network.
[REF5]	eSens Building Blocks - ABB - Capability Lookup - 1.6.0	Capability Lookup is a technical service to accommodate a dynamic and flexible interoperability community. A capability lookup can provide metadata about the communication partner's interoperability capabilities on all levels defined in the European Interoperability Framework.
[REF6]	<i>eSens Building Blocks - PR - SMP</i>	e-SENS will use the SMP (Simple Metadata Publisher) specification originally developed by PEPPOL and generalised and standardised by OASIS. The SMP specification usually complements the Location LookUp ABB.
[REF7]	PEPPOL Transport Infrastructure Service Metadata Publishing (SMP)	This document describes the REST (Representational State Transfer) interface for Service Metadata Publication within the Business Document Exchange Network (BUSDOX).
[REF8]	SML/SMP/eDelivery PKI Impact Assessment for the CEF eHealth DSI	Objectives: 1) Assess the impact of migrating the "Configuration Server" of epSOS to the "SML/SMP" architecture of the eDelivery DSI; 2) Assess the impact of migrating the trust model of epSOS to the eDelivery dedicated PKI; 3) Assess the impacts of the replacement of the VPN network with TESTA services from a technical viewpoint.
[REF9]	Business Document Exchange Network - Common Definitions, CommonDefinitions.pdf	This document contains the definitions and terms that are common between the Business Document Exchange Network (BUSDOX) service metadata and transport specifications. These are: 1° The START and LIME transport specifications; 2° The SML (Service Metadata Locator) and SMP (Service Metadata Publishing) specifications; 3° A scheme for process identifiers. This scheme is identified by the

#	Document	Contents outline
		string —cenbii_procid_pia.
[REF10]	Business Document Metadata Service Location - Software Architecture Document	This document is the Software Architecture document of the CIPA eDelivery Business Document Metadata Service Location application (BDMSL) sample implementation. It intends to provide detailed information about the project: 1) An overview of the solution 2) The different layers 3) The principles governing its software architecture.
[REF11]	PEPPOL Transport Infrastructure Service Metadata Locator (SML)	This document defines the profiles for the discovery and management interfaces for the Business Document Exchange Network (BUSDOX) Service Metadata Locator service.
[REF12]	<i>OASIS - Service Metadata Publishing (SMP) Version 2.0</i>	This document describes the version 2.0 of the Oasis SMP standard.

Important note: documents **listed in bold italic red** in the above list are to be considered for the detailed design and the implementation of the SMP as this one must be fully compliant to those specifications.

2. INTERFACE DEFINITION

2.1. Positioning SMP in eDelivery

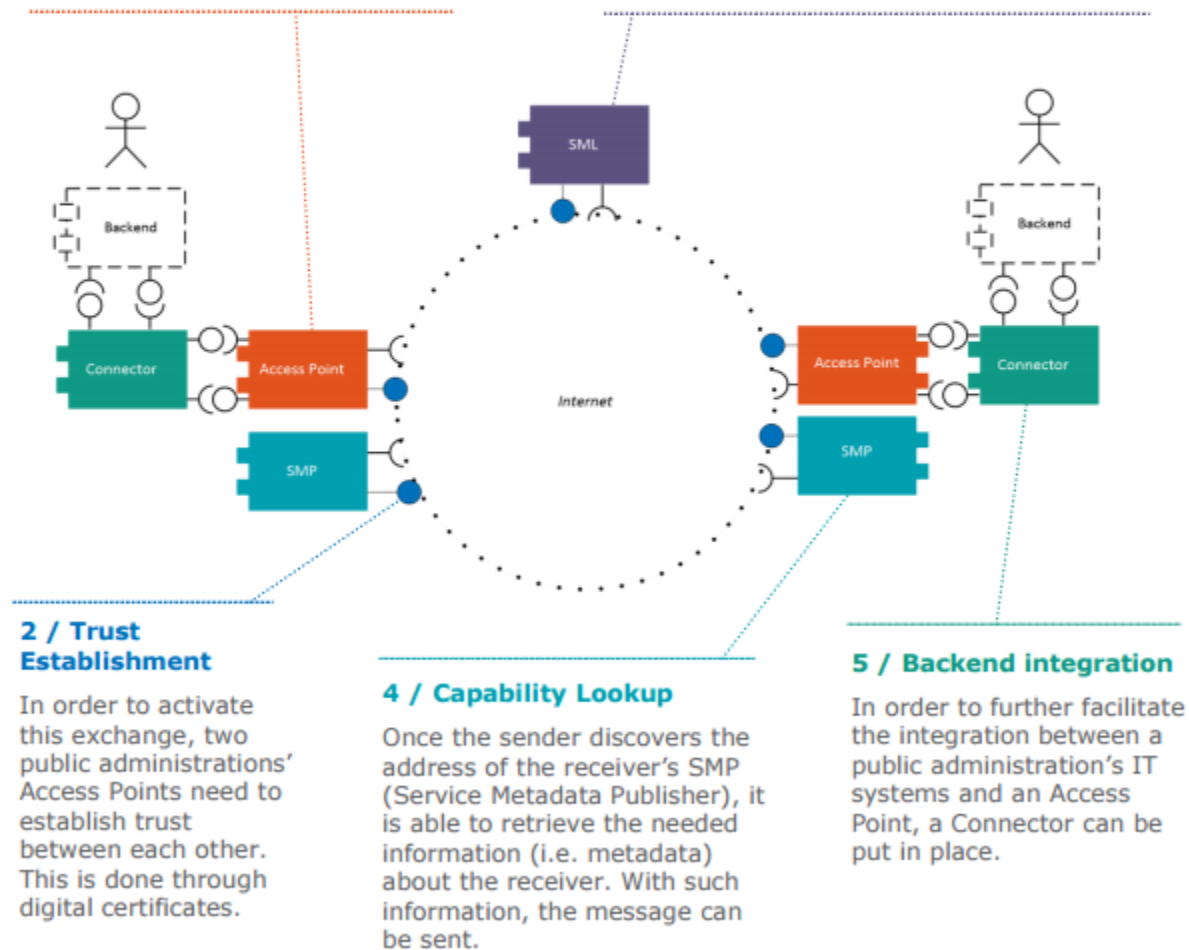
2.1.1. *eDelivery in a nutshell*

1 / Message exchange

At its core, public administrations adopting the same eDelivery Building Block can easily and safely exchange data with each other - even if their IT systems are independent from each other - through an Access Point.

3 / Dynamic Service Location

In order to send a message, a sender needs to discover where the information about a receiver is stored. The SML (Service Metadata Locator) serves this purpose, and guides the sender towards this location, which is called SMP (Service Metadata Publisher).



2 / Trust Establishment

In order to activate this exchange, two public administrations' Access Points need to establish trust between each other. This is done through digital certificates.

4 / Capability Lookup

Once the sender discovers the address of the receiver's SMP (Service Metadata Publisher), it is able to retrieve the needed information (i.e. metadata) about the receiver. With such information, the message can be sent.

5 / Backend integration

In order to further facilitate the integration between a public administration's IT systems and an Access Point, a Connector can be put in place.

Figure 1 – eDelivery components

The technical architecture of eDelivery is based on a conceptual model called '**four-corner model**'. This means that Backend systems (corners one and four) do not exchange messages directly with each other but via Access Points (corners two and three) that, in any given exchange, play the sender or receiver role.

The Access Points of eDelivery are not operated centrally, instead they are deployed in the Member States under the responsibility of a public or private sector service provider.

The users of the Access Points are the Backend systems that need to exchange information with other administrations or businesses across borders.

During the exchange, the data and documents are secured by eDelivery's trust establishment mechanisms. This implies a choice of trust establishment model.

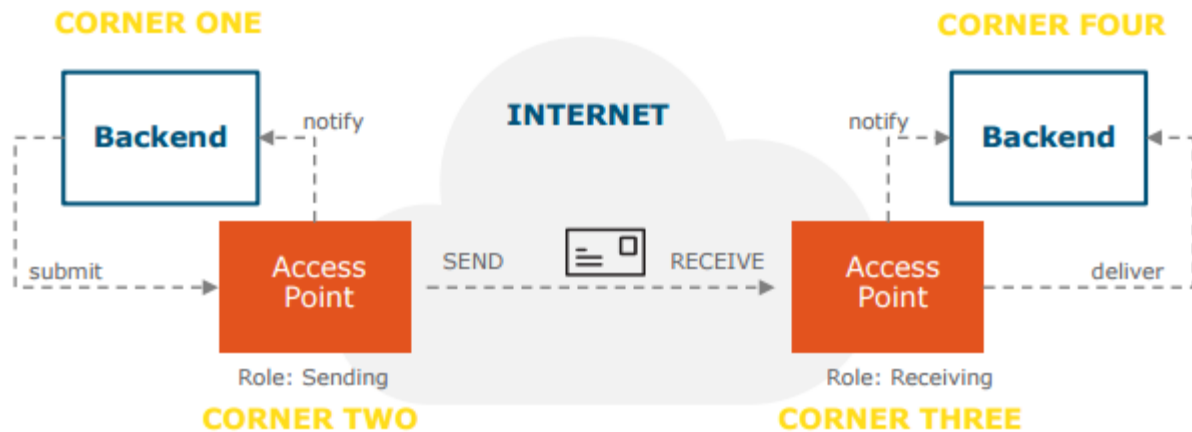


Figure 2 - The four corner model

2.1.2. SMP role

The role of the SMP in the 'four corner model' is

- on one hand to allow servers (*receivers*) to publish the definition of the services they provide, i.e., the documents they are able to receive and the means through which they can receive them,
- on the other hand, to allow clients (*senders*) to find out the definitions of those services.

In that purpose, the SMP will provide services respectively to register services definitions (like "put metadata") by the receiver's administrator and to consult those definitions ("Retrieve Metadata") by the sender.

2.1.3. SMP / SML interactions

In order for the complete process to be consistent, the SMP must propagate some information to the SML:

- The location information of the SMP itself for allowing the senders to discover the SMP
- The location information of all access points providing access to the declared ServiceGroups of the participants the SMP is managing.

In that purpose, the SML exposes several management services that allow the SMP to declare new location information or changes upon existing one. These management interfaces are introduced in [REF11], and are listed below:

- **“Manage participant identifiers”** interface. This is the interface for Service Metadata publishers for managing the metadata relating to specific participant identifiers that they make available.
- **“Manage service metadata”** interface. This is the interface for Service Metadata publishers for managing the metadata about their services, e.g., binding, interface profile and key information.

These interfaces will not be detailed here but the document will refer to these when they are invoked from the SMP REST services. Refer to the *“Execution”* sections of the REST Services definitions below for further details on these interactions.

In addition, the SML exposes the Service Metadata discovery interface. This is the lookup interface which enables senders to discover service metadata about specific target participants. As it is out of the scope of this document this service is not further discussed in the present document.

This functionality is currently not addressed but should be in a future release. The following use cases should then be foreseen:

- UC08 - Register SMP
- UC09 - Change SMP Location
- UC10 - Unregister SMP
- UC11 - Migrate Metadata SMP

2.2. Data model

The SMP interface is built around the data it is intended to manage. Therefore, this document starts by defining the data itself.

2.2.1. Logical data model

The diagram below depicts the major parts of the data model describing the configuration held by the SMP and managed through the interface described in this document. This model is another view of the XSD definition that can be found in annex 3.1 – "XSD files"

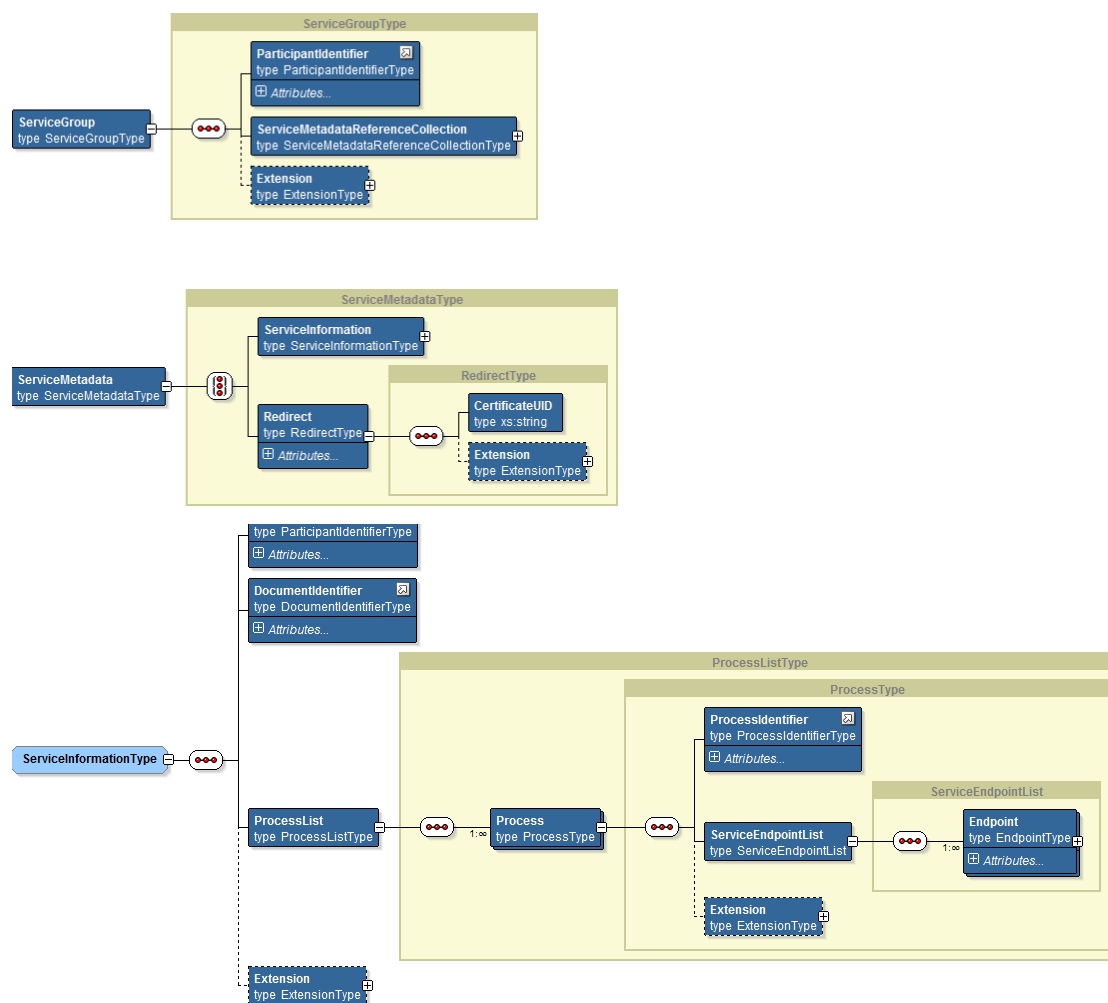


Figure 3- Logical data model (high level view)

2.2.1.1. ServiceGroup

A service group is defined as “structure that represents a set of services associated with a specific **Participant identifier** that is handled by a specific Service Metadata Publisher. The ServiceGroup structure holds a list of references to ServiceMetadata resources in the ServiceList structure”. (cf. [REF7], Data model)

Refer to [REF4] § 2.4 “Identifiers” for Oasis SMP 1.0 or [REF11] § 3.0 “Identifiers” for Oasis SMP 2.0 to find more details and additional references about identifiers of participants (/businesses), documents and processes.

2.2.1.2. ServiceMetadata

ServiceMetadata is defined as “a structure that represents *Metadata* about a specific *electronic service*. The role of the ServiceMetadata structure is to associate a participant identifier with the ability to receive a specific document type over a specific transport [...]”

Refer to [REF4] § 2.4 “Identifiers” for Oasis SMP 1.0 or [REF11] § 3.0 “Identifiers” for Oasis SMP 2.0 to find more details and additional references about identifiers of participants (/businesses), documents and processes.

2.2.1.3. Process

As stated above, a ServiceMetadata is defined as “a structure that represents *Metadata* about a specific *electronic service*. The role of the ServiceMetadata structure is to associate a participant identifier with the ability to receive a specific document type over a specific transport.”

But...

“It also describes *which business processes a document can participate [...]*” (cf. [REF7], “Data model”)

... and it is the purpose of this intermediate entity (*Process*) to hold the process-related information (i.e. its identifier and scheme), and to allow a participant to use a document type to participate in multiple business processes (when applicable).

2.2.1.4. Endpoint

The endpoint is the ultimate entity, holding all the necessary information for all services of the ServiceGroup to be accessed by the sender in order to send document(s) to the receiver (cf. § 2.3.4.4 “Description of the individual fields (elements and attributes)” of [REF4] and [REF11])

XSD element	Description
<p>endpointURI</p> <p>Oasis SMP 1.0 Element :</p> <p>/ServiceEndpointList/ Endpoint/EndpointURI</p> <p>Oasis SMP 2.0 Element:</p> <p>/sma:ProcessMetadata/sma:Endpoint/smb:AddressURI</p>	<p>The address of an endpoint, as a URL</p>
<p>transportProfile</p> <p>Oasis SMP 1.0 Element :</p> <p>ServiceInformation/ ProcessList/./Endpoint/ @transportProfile</p> <p>Oasis SMP 2.0 Element:</p> <p>/ServiceMetadata/sma:ProcessMetadata/sma:Endpoint/smb:TransportProfileID</p>	<p>Indicates the type of transport method that is being used between access points</p>

XSD element	Description
<p>requireBusinessLevelSignature</p> <p>Oasis SMP 1.0 Element :</p> <p>ServiceInformation/ ProcessList/./Endpoint/ RequireBusinessLevelSignature</p> <p>Oasis SMP 2.0 Element: /</p>	<p>Set to “true” if the recipient requires business-level signatures for the message, meaning a signature applied to the business message before the message is put on the transport. This is independent of the transport-level signatures that a specific transport profile might mandate. This flag does not indicate which type of business-level signature might be required. Setting or consuming business-level signatures would typically be the responsibility of the final senders and receivers of messages, rather than a set of gateways.</p>
<p>minimumAuthenticationLevel</p> <p>Oasis SMP 1.0 Element :</p> <p>ServiceInformation/ ProcessList/./Endpoint/ MinimumAuthenticationLevel</p> <p>Oasis SMP 2.0 Element: /</p>	<p>Indicates the minimum authentication level that recipient requires. The specific semantics of this field is defined in a specific instance of a 4-corner infrastructure.</p>
<p>serviceActivationDate</p> <p>Oasis SMP 1.0 Element :</p> <p>ServiceInformation/ ProcessList/./Endpoint/ ServiceActivationDate</p> <p>Oasis SMP 2.0 Element: sma:ProcessMetadata/sma:Endpoint/smb:ActivationDate</p>	<p>Activation date of the service. Senders should ignore services that are not yet activated. Format of ServiceActivationDate date is xs: dateTime.</p>

XSD element	Description
<p>serviceExpirationDate</p> <p>Oasis SMP 1.0 Element : /ProcessList/./Endpoint/ ServiceExpirationDate</p> <p>Oasis SMP 2.0 Element: sma:ProcessMetadata/sma:Endpoint/smb:ExpirationDate</p>	<p>Expiration date of the service. Senders should ignore services that are expired.</p> <p>Format of ServiceExpirationDate date is xs:dateTime.</p>
<p>certificate</p> <p>Oasis SMP 1.0 Element : /ProcessList/./Endpoint/ Certificate</p> <p>Oasis SMP 2.0 Element: /ServiceMetadata/sma:ProcessMetadata/sma:Endpoint/sma:Certificate</p>	<p>Holds the complete [X509v3] signing certificate of the recipient gateway, as a PEM base 64 encoded DER formatted value.</p>
<p>serviceDescription</p> <p>Oasis SMP 1.0 Element : /ProcessList/./Endpoint/ ServiceDescription</p> <p>Oasis SMP 2.0 Element: /</p>	<p>A human readable description of the service</p>
<p>technicalContactUrl</p> <p>Oasis SMP 1.0 Element : /ProcessList/./Endpoint/ TechnicalContactUrl</p> <p>Oasis SMP 2.0 Element: /ServiceMetadata/sma:ProcessMetadata/sma:Endpoint/smb>Contact</p>	<p>Represents a link to human readable contact information. This might also be an email address.</p>
<p>technicalInformationUrl</p> <p>Oasis SMP 1.0 Element : /ProcessList/./Endpoint/ TechnicalInformationUrl</p>	<p>A URL to human readable documentation of the service format. This could for example be a web site containing links to XML Schemas,</p>

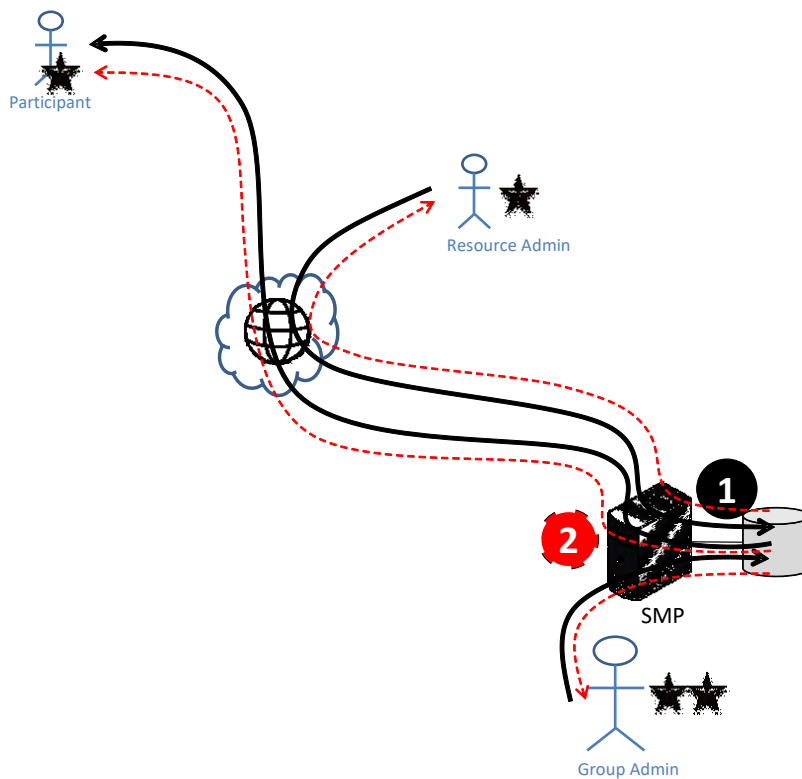
XSD element	Description
Oasis SMP 2.0 Element:	WSDLs, Schematrons and other relevant resources.
extension Oasis SMP 1.0 Element : /Process/Extension Oasis SMP 2.0 Element: /ServiceMetadata/sma:ProcessMetadata/ext:SMPExtensions	The extension element may contain any XML element. Clients MAY ignore this element. It can be used to add extension metadata to the process metadata block as a whole.
extension Oasis SMP 1.0 Element : /ServiceInformation/ Extension Oasis SMP 2.0 Element: /	The extension element may contain any XML element. Clients MAY ignore this element. It can be used to add extension metadata to the service metadata.

Table 1 - XSD elements

2.2.2. XSD files

Two XSDs are used to support the overall processes as defined in §2.6.1.1 - "Administration process":

1. The first one is the 'standard' one as published by OASIS which defines the interface for the storage and the retrieval of participant's information (cf. §3.1.1 – "Original official OASIS SMP XSD").
2. The second one, defined in this document (cf. 3.1.2 – "Extended SMP XSD ") defines the structure of error messages.



2.3. Use cases summary

2.3.1. Actors





Actor	Definition
System Admin 	<p>A user granted rights to administer the Domain Admin type of users.</p> <p>This role is symbolised by 4 stars (it has the highest authority). The system admin is application role with permissions to configure SMP systems settings.</p>
Domain Admin 	<p>A user granted to administer the Domain groups. The domain groups are group of users in the domain/network. The user can create/delete groups and manage the memberships of the groups.</p> <p>The role is symbolised by 3 stars (it has the authority to create/delete and assign the Group admin users to the groups)</p>
Group Admin 	<p>A user granted rights to administer the participants for the group. The group admin administers the resources (Service groups) and assigns the memberships to the resources.</p> <p>This role is symbolised by 2 stars (it has the authority to create/delete resources (ServiceGroups) and to assign the admin users to the resources)</p>
Resource Admin 	<p>A user granted rights to administer the national access points (i.e. one or more ServiceGroups); i.e. to define the access points services metadata.</p> <p>This role is symbolised by 1 single stars (it has the authority to administer (update) the resource (service groups) and subresources (ServiceMetadata), but cannot create or delete the resource)</p>
User	<p>Any participant sending documents to any other receiver participant and consulting the SMP in that purpose</p> <p>This role is symbolised by no single star since he has only public read accesses</p>

Table 2 – Actors

In addition to the role described above, the two additional terms will be used:

- **Sender:** to refer to an actor who uses the system (the SMP) on the left hand side of the ‘four corner model’ introduced in 2.1.1 – “eDelivery in a nutshell”. In the present use cases, the sender will only behave as a ‘User’ as described above in the roles list.
- **Receiver:** to refer to an actor who uses the system (the SMP) on the right hand side of the same model. In the present use cases, the receiver will behave as “Resource Admin.

The “System Admin” being neither on the left nor on the right of that model, but rather on top of it, he will never be referred to as ‘sender’ nor ‘receiver’.

2.3.2. Use cases diagram

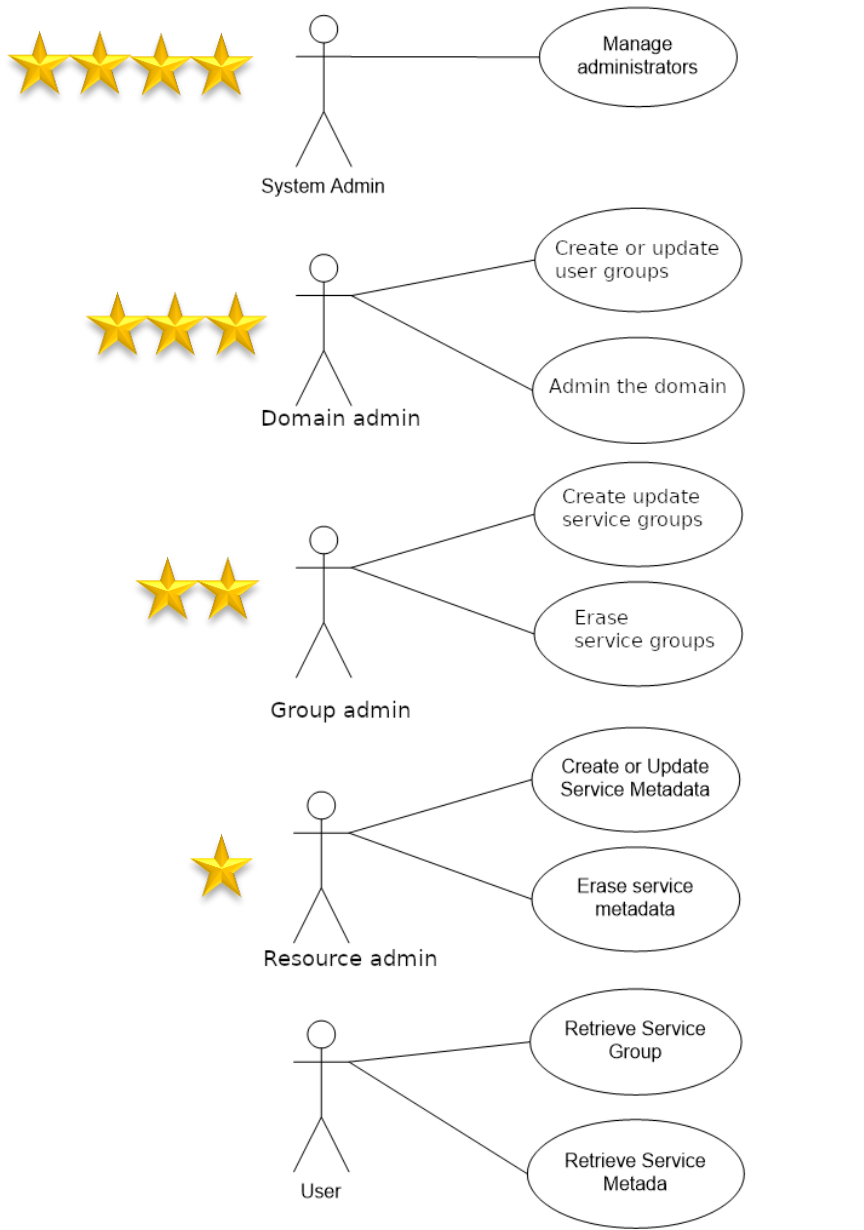


Figure 4- Use cases diagram

2.3.3. Use case list

ID	Actor	UC	Short description	Oper.	Data
UC01	System Admin	Manage Administrators	Create and modify user information i' SMP table 'A'ministrator'	n/a	User (table)
UC02	Group Admin	Create or Update Resources/Service Group	Create a new ServiceGroup for a new receiver participant. This service stores the <i>Service Group</i> and links it to the specified duplet participantIdentifier + participantIdentifierScheme. Information is store into ServiceGroup table. This same service is used to create and update a ServiceGroup.	PUT	ServiceGroup
UC03	Group Admin	Erase Resource/Service Group	Erases the service group definition AND the list of services for the specified receiver participant.	DELETE	ServiceGroup
UC04	Resource Admin	Create or Update Service Metadata	Publish detailed information about one specific document service (multiple processes and endpoints). This same service is used to create and update ServiceMetaData.	PUT	ServiceMetadata
UC05	Resource Admin	Erase Service Metadata	Remove all information about one specific service (i.e. all related processes and endpoints definitions)	DELETE	ServiceMetadata
UC06	User	Retrieve Service Group	Obtain the list of services provided by a specific receiver participant (collection of references to the ServiceMetaData's) This service provides the information related to the <i>Service Group</i> according to the input duplet participantIdentifier + participantIdentifierScheme. Returns information from the ServiceMetadata table only (references to actual MetaData).	GET	ServiceGroup

ID	Actor	UC	Short description	Oper.	Data
UC07	User	Retrieve Service Metadata	Obtain detailed definition about one specific service of a specific participant for all supported transport. This service retrieves the SignedServiceMetadata according to the input quadruplet participantIdentifier+participantIdentifierScheme+documentIdentifier+documentIdentifierScheme. Returns information from the Endpoint table.	GET	SignedServiceMetadata

Table 3 – Use cases list

2.3.4. Story

The following “story” shows a typical example of successive usage of the use cases (when applicable) as it might happen in real life. Each step of this story is prefixed with the use case identifier if the SMP (the System) is involved. If ‘N/A’ is mentioned, some action part of the ‘story’ happens without any involvement of the SMP.

- UC01: As "System Admin", I create a new 'Group Admin' to allow the creation and the management of a new ServiceGroup for a participant.
- UC01: As "System Admin", I create a new 'Resource Admin' to allow the creation and the management of the metadata of that new ServiceGroup.
- UC02: As "Group Admin", I create a new ServiceGroup and link it to the administrator “Resource Admin” to allow the management of ServiceMetadata for the related participant.
- UC04: As "Resource Admin", I define ALL the ServiceMetadata for the participant that I administer.
- N/A: As "User", I ask the DNS to resolve the address of the SMP hosting the receiver's metadata.
- UC07: As "User", I retrieve the definition of the service (metadata) I need to invoke to send a document to the receiver.
- N/A: As "User", I send the document to the receiver.

2.4. Administration use cases

Paragraphs 2.4 and 2.5 define the use cases listed above with more detail.

The following use cases (of this paragraph 2.4) are intended for the different types of administrators in order to define all services (*ServiceGroup* and *ServiceMetada*).

2.4.1. UC01 - Manage Administrators

This use case introduces the foundation for an administration console: creating an 'Group Admin' user is the task of superuser, and no REST service shall consequently support that functionality. As this is a necessary functionality, this one should be included into the administration console.

2.4.1.1. Use Case

Brief description

Create and modify administrator information in SMP table 'Administrator'.

Note: this temporary solution will later be replaced by functionality in a user-friendly administration console.

Actors

System Admin

Preconditions

The actor (system admin) has all access rights to modify content of SMP configuration tables

Basic flow event

Step

- 1 System admin creates a new administrator in table 'Administrator'
- 2 Use case ends with success

Alternative flows

1a **Administrator must be removed**

1a1 System admin removes all ServiceGroup definitions linked to that administrator by calling "DeleteServiceGroup" SMP service for all ServiceGroups this administrator is linked to (as defined by the "ownership" relationship).

1a2 System admin removes the administrator from table 'Administrator'

1b **New administrator must take over administration of some participant(s)**

1b1 After creating the new user (step 1), the system admin reassigns specific ServiceGroups to that user by changing the 'username' foreign key in table Ownership.

1b2 Use case ends

1c **Administrator already exists and must be modified**

1c1 System admin modifies some data (role, password) of the user in table 'User'

1c2 Use case ends

Post conditions

Successful conditions

Administrator definition has been modified

Failure conditions

N/A

2.4.1.2. REST Service: None

This functionality should be implemented into the administrator's console of the SMP which is not further detailed in the present document.

2.4.2. UC02 - Create or Update Service Group

2.4.2.1. Use case

Brief description

Create a new ServiceGroup for a new receiver participant.

This service stores the Service Group and links it to the specified duplet participantIdentifier + participantIdentifierScheme.

Information is stored into ServiceGroup table.

This same service is used to create and update a ServiceGroup.

Actors

Group Admin

Preconditions

The authenticated user has the role of " Group Admin"

If the ServiceGroup is managed remotely, the "Resource Admin" must have been created before in the "Administrator" table.

Identifier and scheme of the service group provided in the request must comply to the policy defined in [REF3]

If the SMP is serving multiple domains, the header field "Domain" must be populated and refer to one of the domains served by the SMP.

Basic flow event

Step

- 1 The receiver declares its service group and the related Administrator (Resource Admin) to the SMP
- 2 The SMP authenticates the user, validates the request, and add or replace the information into its configuration database and passes the information to the SML.
- 3 The receiver receives the confirmation that the definitions were stored properly with HTTP response "201 Created".
- 4 Use case ends with success

Alternative flows

- 3a **ServiceGroup already exists**
- 3a1 The receiver receives the confirmation that the definitions were updated properly with HTTP response "200 OK".
- 3a2 Use case ends with success

Exception flows

- 1a **SMP is not reachable**
- 1a1 The user receives a network connection error
- 1a2 Use case ends

- 2a **Authentication / authorization fails**
- 2a1 The SMP replies with HTTP error "401 Unauthorized"
- 2a2 The receiver receives the error message

- 2a3 Use case ends
- 2b **Request is not well formed (or any other business/technical error)**
- 2b1 The SMP replies with HTTP error "400 Bad request" or "500 Internal server error" with details on the error allowing to identify the error in the request (cf. "Error codes" table below)
- 2b2 The receiver receives the error message
- 2b3 Use case ends
- 2c **SMP is serving multiple domains and the Domain field is not specified in the header**
- 2c1 The SMP replies with HTTP error "400 Bad request" (business code WRONG_FIELD) with message: "SMP is configured to use multiple domains, but no Domain is specified in request. Please specify Domain in request."
- 2c2 The receiver receives the error message
- 2c3 Use case ends
- 2d **Domain field refers to a domain that is not served by the SMP**
- 2d1 The SMP replies with HTTP error "400 Bad request" (business code WRONG_FIELD) with message: "Requested domain does not exist " (followed by the domain field value)
- 2d2 The receiver receives the error message
- 2d3 Use case ends

Post conditions

Successful conditions

ServiceGroup is either created or updated, and the corresponding "Resource Admin" is defined.

Failure conditions

In case of error, no change occurs into the configuration database and the response gives technical details on the exception condition

2.4.2.2. REST Service: PutServiceGroup

Input:

- **In the URL:**
 - The participant's identifier and identifier's scheme (ParticipantIdentifier)
- **In the header (optional fields):**
 - the Certificate Identifier required for authenticating the remote user as "Resource Admin" for this service group.

NB: if the Certificate Identifier is not provided, the "Group Admin " will manage the metadata of that Service Group – the username of the basic authentication is used to identify the "Group Admin " to link him with the Service Group.

- The "Domain" for which the ServiceGroup must be created.

NB: this field is optional and relevant only if the SMP is serving multiple domains. In that case this field must be provided.

- **In the TEXT:** a ServiceGroup structure as defined in the standard OASIS XSD (cf. 3.1.1 - "Original official OASIS SMP XSD") containing:
 - The Participant's identifier and scheme that uniquely identifies this service group; These must be identical to the ones provided in the URL.
 - Optionally, the Extension information in the HTTP TEXT

Details on the *ServiceGroup-Owner* structure:

- The following attributes of the certificate will be used in this order:
 - CN,
 - O,
 - C, and
 - Serial number
- As an example, the following certificate:

```
sno=0001&subject=EMAILADDRESS=receiver@test.be, CN=SMP_receiverCN,
OU=B4, O=DIGIT, L=Brussels, ST=BE, C=BE:df48f09389f034&validfrom=Jun 1
10:37:53 2015 CEST&validto=Jun 1 10:37:53 2035
CEST&issuer=EMAILADDRESS=root@test.be,CN=rootCN,OU=B4,O=DIGIT,L=Brussels,
ST=BE,C=BE
```

will be provided as such in the HTTP header:

ServiceGroup-Owner: CN=SMP_receiverCN, O=DIGIT, C=BE:df48f09389f034

Execution:

- Start a new transaction.
- Create or update (overwrites) the corresponding rows in the configuration, ownership and ServiceGroup identified by the participant's identifier and identifier's scheme keys:

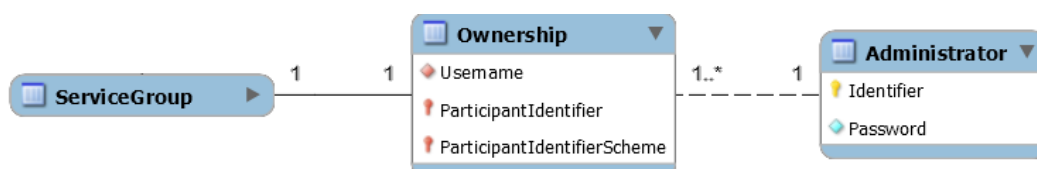


Figure 5- ServiceGroup data model

- If attribute *ServiceGroup-Owner* is present in the HTTP Header, then use this as information to store as "Identifier"
- If not, store instead the basic authentication information provided in the HTTP header.
- If it is a newly created ServiceGroup, invoke SML service "Create Business Identifier".

- If it is an existing ServiceGroup, invoke SML services "Delete Business Identifier" and then "Create Business Identifier".
- If SML service invocation succeeded, commit the transaction.
- If SML service invocation failed:
 - rollback the transaction;
 - if necessary (delete succeeded), try to re-invoke "Create Business Identifier" with the old information to restore the SML properly;
 - Response to this service is "failure".

Output:

Return a response confirming the success (or eventually the failure) of the operation.

Sample Request

HTTP Header (No AdminServiceGroup authentication information – Group Admin creates or updates the ServiceGroup)

```
PUT http://smp-digit-mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu/ehealth-actorid-
qns::urn:poland:ncpb HTTP/1.1
Host: smp-digit-mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu
Accept: application/xml
Content-Type: application/xml
Authorization: Basic dXNlcjpwYXNz
Content-Length: 278
```

HTTP Header (Resource Admin authentication information is certificate)

```
Host: smp-digit-mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu
Accept: application/xml
Content-Type: application/xml
ServiceGroup-Owner: CN=SMP_1000000181,O=DIGIT,C=DK:406b2abf0bd1d46ac4292efee597d414
Authorization: Basic dXNlcjpwYXNz
Content-Length: 278
```

Text

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<ServiceGroup xmlns="http://docs.oasis-open.org/bdxc/ns/SMP/2016/05">
  <ParticipantIdentifier scheme="ehealth-actorid-qns">urn:poland:ncpb</ParticipantIdentifier>
  <ServiceMetadataReferenceCollection/>
</ServiceGroup>
```

Sample Response

HTTP header

```
HTTP/1.1 201 Created
Server: Apache-Coyote/1.1
Pragma: No-cache
Expires: Thu, 01 Jan 1970 01:00:00 CET
Content-Length: 0
Date: Wed, 27 Jan 2016 10:32:40 GMT
Cache-Control: no-cache, proxy-revalidate
Connection: Keep-Alive
```

NB: if the ServiceGroup previously existed, "200 OK" will be returned as HTTP response instead of "201 Created" as showed in the above example.

Text

N/A.

Error codes

HTTP code	HTTP Message	Business code	Meaning
200	OK	n/a	The request was completed successfully.
201	Created	n/a	The PUT operation completed successfully.
400	Bad Request	XSD_INVALID	The XML included in the request is not validate against the XSD defining the input structure.
400	Bad Request	MISSING_FIELD	Some field that is optional in the XSD but mandatory for this invocation is missing (missing field name in description).
400	Bad Request	WRONG_FIELD	Some field is valid against XSD definition, but the more specific content is invalid (erroneous field name in description). Or Some header field is either missing or invalid.
400	Bad Request	FORMAT_ERROR	Some field is expected to have a specific format is not valid (erroneous field name in description).
400	Bad Request	USER_NOT_FOUND	The referenced " Resource Admin" was not found as Administrator.
401	Unauthorized	UNAUTHORIZED	The user is not granted the right to issue this request.
404	Resource not found	NOT_FOUND	The requested information was not found.
500	Internal Server Error	TECHNICAL	Some unexpected technical error occurred (detailed information is available in the response).

Table 4 – UC02 Error codes

NB: the business code and the description are in the response and compliant to the ErrorResponse type as described in §3.3 – "Detailed Errors structure".

Audit

The following information must be audited for this service (more details under §2.6.5 – 'Auditing'):

- AdministratorIdentifier
- AccessTime
- Operation
- ParticipantIdentifier
- ParticipantIdentifierScheme
- IpAddress
- RequestHeader
- RequestText
- ResponseHeader
- HTTP code
- Business code
- ErrorDescription

2.4.3. UC03 - Erase Service Group

2.4.3.1. Use case

Brief description

Erases the service group definition AND the list of services for the specified receiver participant.

Actors

Group Admin

Preconditions

The authenticated user has the role of " Group Admin".

Referenced service group was previously defined.

Basic flow event

Step

- 1 The receiver requests its service group to be removed from the SMP.
- 2 The SMP authenticates the user, validates the request, and removes all the information on the service group from its configuration and from the SML.
- 3 The receiver receives the confirmation that the definitions were removed properly with HTTP response "200 OK".
- 4 Use case ends with success.

Exception flows

1a **SMP is not reachable**

- 1a1 The user receives a network connection error.
- 1a2 Use case ends.

2a **Authentication / authorization fails**

- 2a1 The SMP replies with HTTP error "401 Unauthorized".
- 2a2 The receiver receives the error message.
- 2a3 Use case ends.

2b **Request is not well formed (or any other business/technical error)**

- 2b1 The SMP replies with HTTP error "400 Bad request" or "500 Internal server error" with details on the error allowing to identify the error in the request (cf. "Error codes" table below).
- 2b2 The receiver receives the error message.
- 2b3 Use case ends.

2c **ServiceGroup is not defined**

- 2c1 The SMP replies with HTTP error "404 Resource not found".
- 2c2 The receiver receives the error message.
- 2c3 Use case ends.

Post conditions

Successful conditions

The specified service group is removed with all its related information.

Failure conditions

In case of error, no change occurs into the configuration database and the response gives technical details on the exception condition.

2.4.3.2. REST Service: DeleteServiceGroup

Input: ServiceGroup identifier: ParticipantIdentifier, ParticipantIdentifierScheme in the HTTP header

Execution:

The username or the certificate from the HTTP header is verified to be the owner of the specified Service Group. If not, the operation is rejected.

Start a new transaction.

Delete ALL information related to that service group in tables: Endpoint, Process, ServiceMetadata and finally the ServiceGroup itself where the *ParticipantIdentifiers* match the specified *ServiceGroup* identifier.

Invoke SML service “Delete Business Identifier”.

If SML service invocation succeeded, commit the transaction.

If SML service invocation failed:

- rollback the transaction;
- Response to this service is “failure”.

Output: HTTP 200 if done, 404 if the specified service group does not exist and 500 if any error occurred.

Sample Request

HTTP Header

```
DELETE http://smp-digit-mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu/ehealth-actorid-
qns::urn:poland:ncpb HTTP/1.1
Host: smp-digit-mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: application/xml
Accept-Language: en-GB,en;q=0.8,de;q=0.5,fr;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://130.206.118.4/smp-swagger-ui/
Origin: http://130.206.118.4
Proxy-Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Connection: keep-alive
```

Text

N/A

Sample Response

HTTP header

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 20
Content-Type: application/xml
Date: Thu, 22 Dec 2016 10:47:56 GMT
Server: Jetty(6.1.26)
Set-Cookie: BCIDSLB=PS1LUX-56; domain=europa.eu; path=/; HttpOnly
access-control-allow-origin:*
```

Text

N/A

Error codes

HTTP code	HTTP Message	Business code	Meaning
200	OK	n/a	The request was completed successfully
400	Bad Request	FORMAT_ERROR	Some field is expected to have a specific format is not valid (erroneous field name in description)
401	Unauthorized	UNAUTHORIZED	The user is not granted the right to issue this request
404	Resource not found	NOT_FOUND	The requested information was not found
500	Internal Server Error	TECHNICAL	Some unexpected technical error occurred (detailed information is available in the response)

Table 5 – UC03 Error codes

Audit

The following information must be audited for this service (more details under §2.6.5 – 'Auditing'):

- AdministratorIdentifier
- AccessTime
- Operation
- ParticipantIdentifier
- ParticipantIdentifierScheme
- IpAddress
- RequestHeader
- ResponseHeader
- HTTP code
- Business code
- ErrorDescription

2.4.4. UC04 - Create or Update Service Metadata

2.4.4.1. Use case

Brief description

Publish detailed information about one specific document service (multiple processes and endpoints).

This same service is used to create and update ServiceMetadata.

(Cf. [REF7] §2.1) A sender (ed. "user") may want to discover what document types can be handled by a specific participant identifier. Such discovery is relevant for applications supporting several equivalent business processes. Knowing the capabilities of the recipient is valuable information to a sender application and ultimately to an end user. E.g., the end user may be presented with a choice between a "simple" and a "rich" business process.

This is enabled by a pattern where the sender first retrieves the ServiceGroup entity, which holds a list of references to the ServiceMetadata resources associated with it. The ServiceMetadata in turn holds the metadata information that describes the capabilities associated with the recipient participant identifier

Actors

Resource Admin

Preconditions

- The authenticated user has the role of "Resource Admin"
- Resource Admin user initiating the request is linked to the specified ServiceGroup
- The certificate of the "Resource Admin" is valid
- The certificate information of the "Resource Admin" was previously stored in the configuration

Identifier and scheme of the service group and documents provided in the request must comply to the policy defined in [REF3]

Basic flow event

Step

- 1 The receiver requests its service metadata to be put into the SMP.
- 2 The SMP verifies the certificate of the "Resource Admin" against its information in the database, validates the request, and either create or update all the information into its configuration database.
- 3 The receiver receives the confirmation that the definitions were created properly with HTTP response "201 Created".
- 4 Use case ends.

Alternative flows

3a **ServiceMetadata already exists**

- 3a1 The receiver receives the confirmation that the definitions were updated properly with HTTP response "200 OK".
- 3a2 Use case ends with success.

Exception flows

1a **SMP is not reachable**

- 1a1 The user receives a network connection error.
- 1a2 Use case ends with success.

2a **Authentication / authorization fails**

- 2a1 The SMP replies with HTTP error "401 Unauthorized".

2a2 The receiver receives the error message.

2a3 Use case ends.

2b **Request is not well formed (or any other business/technical error)**

- 2b1 The SMP replies with HTTP error "400 Bad request" or "500 Internal server error" with details on the error allowing to identify the error in the request (cf. "Error codes" table below).

2b2 The receiver receives the error message.

2b3 Use case ends.

2c **ServiceGroup is not defined**

- 2c1 The SMP replies with HTTP error "404 Resource not found".

2c2 The receiver receives the error message.

2c3 Use case ends.

Post conditions

Successful conditions

ServiceMetadata is defined0

Failure conditions

In case of error, no change occurs into the configuration database and the response gives technical details on the exception condition.

2.4.4.2. REST Service : PutServiceMetadata

Input:

- ServiceGroup and Document's identifiers in the URL and
- *ServiceMetadata* in the text

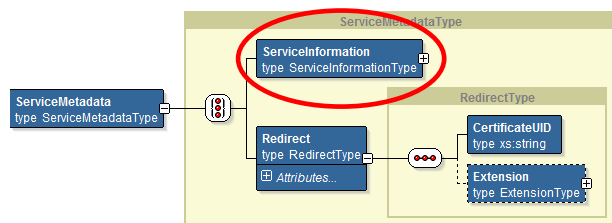


Figure 6- ServiceInformation data model

This input structure, from the *ServiceInformation* node down to the Process leaves, will fully define the content of the referenced service metadata as defined by the four identifiers of the participant AND related specific document.

This means that the configuration of a Service must be done with a single call (for all *Processes*) to this service, and it can be considered that all previously existing information in ServiceInformation, Process and Endpoint tables are discarded (if they exist) and completely replaced by the newly provided information.

Execution:

Start a new transaction.

Insert or replace the all the ServiceInformation for that ServiceGroup Document.

In case of error:

- rollback the transaction
- Response to this service is "failure".

If no error occurred:

- Commit the transaction
- Response to this service is "success".

Authorization

The operation will be allowed if and only if the authenticated user matches the "Resource Admin" user linked to the ServiceGroup.

For this user to be the eligible "Resource Admin" it must have been referenced as such in the ServiceGroup definition (cf. PutServiceGroup) by an "Group Admin" user via service "PutServiceGroup" (by the "Group Admin" who was previously defined by the "Domain Admin").

All the provided information will either be created in the configuration (put = *create*) or be overwritten (put = *update*); i.e., this 'put' operation does both.

Redirection

As explained above, in some cases ServiceMetadata information can be stored in 'another SMP'; i.e., another SMP than the one that is queried by the user. In such case, 'redirect' information is provided to the user to allow him to query the appropriate SMP for obtaining the ServiceMetadata information from the relevant SMP.

For that to be possible, the receiver must eventually be able to store that redirect information. That is why this service provides this possibility, by allowing provision of “Redirect” information instead of the “ServiceInformation” itself:

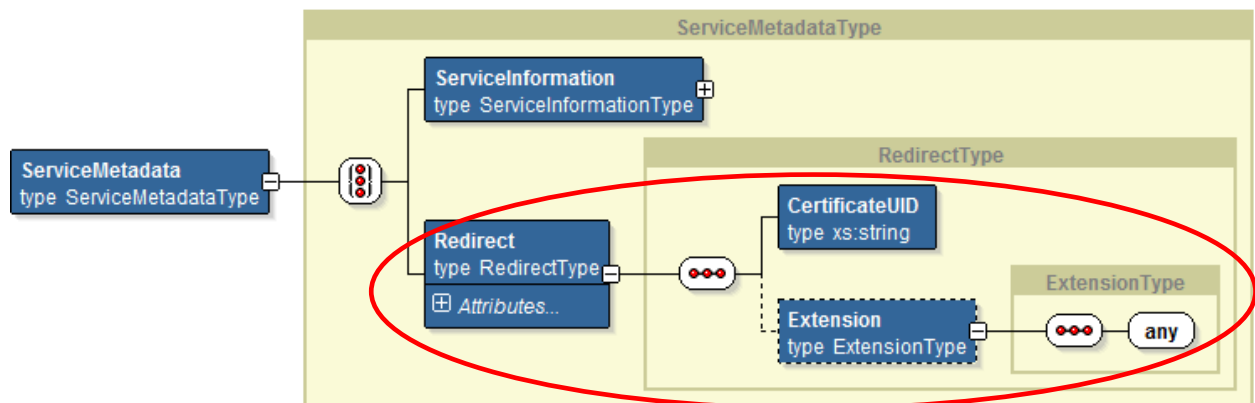


Figure 7- Redirect data model

The fields are in used as follows:

- *CertificateUID*: holds the Subject Unique Identifier of the certificate of the destination SMP. A client SHOULD validate that the Subject Unique Identifier of the certificate used to sign the resource at the destination SMP matches the Subject Unique Identifier published in the redirecting SMP.
- *href* attribute of the Redirect element contains the full address of the destination SMP record that the client is redirected to.
- Extension: not defined and optional.

Note about cascaded redirections:

In the case where a client encounters such a redirection element, the client MUST follow the first redirect reference to the alternative SMP. If the SignedServiceMetadata resource at the alternative SMP also contains a redirection element, the client SHOULD NOT follow that redirect. It is the responsibility of the client to enforce this constraint.

Output: HTTP response code 200 if ok, 401 if not allowed and 400 if any other error occurred. Details are available in the response text.

Sample Request 1

This example sends actual information of the service and uses a certificate in the header.

HTTP Header (with certificate)

```
PUT http://smp-digit-mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu/ehealth-actorid-qns::urn:poland:ncpb/services/ehealth-resid-qns::urn::epsos##services:extended:epsos::107
HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
Client-Cert: sno=0001&subject=EMAILADDRESS=receiver@test.be,CN=SMP_receiverCN,OU=B4,O=DIGIT,L=Brussels,ST=BE,C=BE&validfrom=Jun 1 10:37:53 2015 CEST&validto=Jun 1 10:37:53 2035
CEST&issuer=EMAILADDRESS=root@test.be,CN=rootCN,OU=B4,O=DIGIT,L=Brussels,ST=BE,C=BE

Host: smp-digit-mock.publisher.ehealth.acc.edelivery.tech.ec.europa.eu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: application/xml
```

```

Accept-Language: en-GB,en;q=0.8,de;q=0.5,fr;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/xml
Referer: http://130.206.118.4/smp-swagger-ui/
Content-Length: 4741
Origin: http://130.206.118.4
Proxy-Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
Connection: keep-alive

```

NB: the "Client-Cert" value in the HTTP header above is only an example that is specific to production and acceptance environments at DIGIT and should not be considered as constraining.

Text (Information)

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?><ServiceMetadata
xmlns="http://docs.oasis-open.org/bdxc/ns/SMP/2016/05">
  <ServiceInformation>
    <ParticipantIdentifier scheme="ehealth-actorid-qns">urn:poland:ncpb</ParticipantIdentifier>
    <DocumentIdentifier scheme="ehealth-resid-
qns">urn::epsos##services:extended:epsos::107</DocumentIdentifier>
    <ProcessList>
      <Process>
        <ProcessIdentifier scheme="ehealth-procid-
qns">urn:epsosPatientService::List</ProcessIdentifier>
        <ServiceEndpointList>
          <Endpoint transportProfile="urn:ihe:iti:2013:xcpd">
            <EndpointURI>http://poland.pl/ncp/patient/list</EndpointURI>
            <RequireBusinessLevelSignature>>false</RequireBusinessLevelSignature>
            <MinimumAuthenticationLevel>urn:epSOS:loa:1</MinimumAuthenticationLevel>
            <ServiceActivationDate>2016-06-06T11:06:02.000+02:00</ServiceActivationDate>
            <ServiceExpirationDate>2026-06-06T11:06:02+02:00</ServiceExpirationDate>
          </Endpoint>
        </ServiceEndpointList>
      </Process>
    </ProcessList>
    <Certificate>MIID7jCCA1egAwIBAgICA+YwDQYJKoZIhvcNAQENBQAwojELMAkGA1UEBhMCRIxEzAR
BgNVBAoMCKIIRSBFdXJvcGUxXjAUBgNVBAMMDUIIRSBFdXJvcGUgQ0EwHhcNMTYwNjAxMTQzNTUz
WhcNMjYwNjAxMTQzNTUzWjCBgZELMAkGA1UEBhMCUFQxDDAKBgNVBAoMA01vSDENMAAsGA1UE
CwwEU1BNUzENMAAsGA1UEKgwESm9hbzEOMAwGA1UEBRMFQ3VuaGExHTAbBgNVBAMMFHFhZXB
zb3MubWluLXNhdWRILnB0MRkwFwYDQ0MDBBTZlXj2aWNIIFByb3ZpZGVyMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAE1eN4qPSSRZqjVFG9TlcPlxf2WiSimQK9L1nf9Z/s0ezeGQjCukDeDq/W
zqd9fpHhaMMq+XSSotyEtlr5K/As4kFrViONUUKG12J6UIISWogp0NYFWA4wlqKSFITnQS5/nRTs05oON
CCGILCyJNNe053JzPlaQ3/QbPLssuSAr6XucPE8wBBGM8b/TsB2G/zjG8yuSTgGbhazekq/Vnf9ftj1fr/vJD
DAQgH6Yvzd88Z0DACJPHfW1p4F/OWLI386Bq7g/bo1DUPAyEwlf+CkLgJWRKki3yJI0CIZ9enMA507rfe
G3rXdgYGmWS7tNEgKXxgC+heiYvi7ZWd7M+/SUwIDAQABo4IBMzCCAS8wPgYDVR0fBDcwNTAzoDGg
L4YtaHR0cHM6Ly9nYXplbGxllmloZS5uZXQvcGtPL2Nybc82NDMvY2FjcmwuY3JsMDwGCWCGSAGG+E
IBBAQvFi1odHRwczovL2dhemVsbGUuaWhlLm5ldC9wa2kvY3JsLzY0My9jYWNybc5jcmwwPAYJYIZIAY
b4QgEDBC8WLWh0dHBzOi8vZ2F6ZWxsZS5paGUubmV0L3BraS9jcmwwNjQzL2NhY3JsLmNybcDAfBgNV
HSMEGDAWgBTsMw4TyCJeouFrr0N7el3Sd3MdfjAdBgNVHQ4EFgQU1GQ/K1yklwWFgiOnzWJLQzufF/
8wDAYDVROTAQH/BAIwADAQBgNVHQ8BAf8EBAMCBSAwEwYDVR0lBAwwCgYIKwYBBQUHAWAwEwDQ
YJKoZIhvcNAQENBQADgYEAZ7t1Qkr9wz3q6+WcF6p/YX7Jr0CzVe7w58FvJFk2AsHeYkSIOyO5hxNpQbs
1L1v6JrcqziNFrh2QKGT2v6iPdWtdCT8HBLjmuVvWxxnfzYjdQOJ+kdKMAEV6EtWU78OqL60CctUZKXE/
NKJUq7TTUCFP2fwiAry/t1dTD2NZo8c=</Certificate>
    <ServiceDescription>This is the epsOS Patient Service List for the Polish
NCP</ServiceDescription>
    <TechnicalContactUrl>http://poland.pl/contact</TechnicalContactUrl>
    <TechnicalInformationUrl>http://poland.pl/contact</TechnicalInformationUrl>
  </Endpoint>

```

```

    </ServiceEndpointList>
  </Process>
</ProcessList>
<Extension><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/><SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><Reference
URI=""><Transforms><Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><DigestValue>CJeDJ72nQkwsZ2XWc8ep
ut8pcBzfHSwO6uHr77/xbQo=</DigestValue></Reference></SignedInfo><SignatureValue>WICUwIHJ
y9sehansEjFXSPkAobodbeM8OxXfLjQVYs7Vh085dESYaAbcDoDZ6t8laHbsRtkiCgZG

yVRvOwB42EVRkhyWu0zVnlowfieBgvMqtZdYMBx6Z7Npwvo0UDcYI/HnHnzsyHhkIKKNGPymXJXH

waEt4QJw+ne2n7Tb0Qg=</SignatureValue><KeyInfo><X509Data><X509SubjectName>CN=Sample
National
Infrastructure,OU=Sante,C=PT</X509SubjectName><X509Certificate>MIICAzCCAWygAwIBAgIEWCRz
HjANBgkqhkiG9w0BAQsFADBGMQswCQYDVQQGEwJQVDEOMAwGA1UE

CwwFU2FudGUxZjAlBgNVBAMMHINhbXBsZSBOYXRpb25hbCBJbmZyYXN0cnVjdHVyZTAeFw0xNjEx
MTAxMzE2NTBaFw0yNjExMTAxMzE2NTBaMEYxCzAJBgNVBAYTAIBUMQ4wDAYDVQQQLDAVTYW50ZT
En

MCUGA1UEAwweU2FtcGxllE5hdGlvbmFsIEluZnJhc3RydWN0dXJlMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCywt50WXEWliWytRGcMqzeMM/EyxruNthPdiUEUTbs9un7lzGGjpfFMTgd83wJ
haB6FgpaVd8V2w/JBdkim5Ltuhu2vA0d6hHOsa58neIfe4z1ZhswwNmB0+mDTjwnd/gg8IjYQhhY

c5G4x7m0ZGdDKZDizjtDTEPTsI8D4FzBFwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBACKxUpAx0PYm
ZZi4DfAzBkQ0+CvQw/l6Yo8wonVdpcQXO3khpWlcXhgYhTLHwm8lwJLEyFatmMyCKkISA3CLebJU
L4XH1GcdCg6oPKPUc+ovbgN7/iR265Elp4qHfpVteBijBTyZReH4oAK9hRhK1gLwtjl7vpjVaPXv
vkV1fbrz</X509Certificate></X509Data></KeyInfo></Signature></Extension>
  </ServiceInformation>
</ServiceMetadata>

```


Sample Response (applicable for both examples request above)HTTP header

```
HTTP/1.1 201 Created
Server: Apache-Coyote/1.1
Pragma: No-cache
Expires: Thu, 01 Jan 1970 01:00:00 CET
Content-Length: 0
Date: Fri, 22 Jan 2016 09:46:10 GMT
Cache-Control: no-cache, proxy-revalidate
Connection: Keep-Alive
```

NB: if the ServiceMetadata previously existed, "200 OK" will be returned as HTTP response instead of "201 Created" as show in the above example.

Text

N/A

Error codes

HTTP code	HTTP Message	Business code	Meaning
200	OK	n/a	The request was completed successfully.
201	Created	n/a	The PUT operation completed successfully.
400	Bad Request	XSD_INVALID	The XML included in the request is not validate against the XSD defining the input structure.
400	Bad Request	MISSING_FIELD	Some field that is optional in the XSD but mandatory for this invocation is missing (missing field name in description).
400	Bad Request	WRONG_FIELD	Some field is valid against XSD definition, but the more specific content is invalid (erroneous field name in description).
400	Bad Request	OUT_OF_RANGE	Some numeric (or date field) is out of the valid range (erroneous field name in description).
400	Bad Request	UNAUTHOR_FIELD	Some field that is optional in the XSD but forbidden for this invocation is present (unauthorized field name in description).
400	Bad Request	FORMAT_ERROR	Some field is expected to have a specific format is not valid (erroneous field name in description).
400	Bad Request	OTHER_ERROR	Some other specific error was encountered processing the request (more information in the ErrorDescription field).
401	Unauthorized	UNAUTHORIZED	The user is not granted the right to issue this request.
404	Resource not found	NOT_FOUND	The requested information was not found.
500	Internal Server Error	TECHNICAL	Some unexpected technical error occurred (detailed information is available in the response).

Table 6 – UC04 Error codes

Audit

The following information must be audited for this service (more details under §2.6.5 – 'Auditing'):

- AdministratorIdentifier
- AccessTime
- Operation
- ParticipantIdentifier
- ParticipantIdentifierScheme
- DocumentIdentifier
- DocumentIdentifierScheme
- IpAddress
- RequestHeader
- RequestText
- ResponseHeader
- HTTP code

- Business code
- ErrorDescription

2.4.5. UC05 - Erase Service Metadata

2.4.5.1. Use case

Brief description

Remove all information about one specific service (i.e., all related processes and endpoints definitions).

Actors

Resource Admin (or Group Admin).

Preconditions

The user knows the address of the SMP.

Resource Admin initiating the request is linked to the specified ServiceGroup.

The authenticated user has the role of " Resource Admin".

The referenced ServiceMetadata exists.

Basic flow event

Step

- 1 The receiver requests its service metadata to be removed from the SMP.
- 2 The SMP authenticates the user, validates the request, and delete any information from the referenced ServiceMetadata from its configuration database (from table ServiceMetadata and all its tables).
- 3 The receiver receives the confirmation that the definitions were removed properly with HTTP response "200 OK".
- 4 Use case ends with success.

Exception flows

- 1a **SMP is not reachable**
 - 1a1 The user receives a network connection error
 - 1a2 Use case ends
- 2a **Authentication / authorization fails**
 - 2a1 The SMP replies with HTTP error "401 Unauthorized"
 - 2a2 The receiver receives the error message
 - 2a3 Use case ends
- 2b **Request is not well formed (or any other business/technical error)**
 - 2b1 The SMP replies with HTTP error "400 Bad request" or "500 Internal server error" with details on the error allowing to identify the error in the request (cf. "Error codes" table below)
 - 2b2 The receiver receives the error message
 - 2b3 Use case ends

- 2c **ServiceGroup or ServiceMetadata is not defined**
- 2c1 The SMP replies with HTTP error "404 Resource not found"
- 2c2 The receiver receives the error message
- 2c3 Use case ends

Post conditions

Successful conditions

ServiceMetadata are absent

Failure conditions

In case of error, no change occurs into the configuration database and the response gives technical details on the exception condition

2.4.5.2. REST Service: DeleteServiceMetadata

Input: ServiceMetadata identifier in the HTTP header

Execution:

Authorization

The operation will be allowed if and only the authenticated user matches the "Resource Admin" user linked to the Service Group.

For this user to be the eligible "Resource Admin" it must have been referenced as such in the ServiceGroup definition (cf. PutServiceGroup) by an "Group Admin" user via service "PutServiceGroup".

Start a new transaction.

NB:

If no more ServiceMetadata information is available on the related ServiceGroup, the limited information on the ServiceGroup is nevertheless kept to allow keeping track of the previously defined administrator and the service group. Should it be deleted, it is the responsibility of the "Group Admin" user to issue the required operation (DeleteServiceGroup) if necessary. Delete in one single transaction any information related to that service where participant and documents identifiers match the provided ServiceMetadata identifier.

In case of abort the deletion to undo what was previously done:

- Rollback the transaction
- Response to this service is "failure".

If no error occurred:

- Commit the transaction
- Response to this service is "success".

Output: HTTP 200 if done, 404 if the service metadata or the service group does not exist and 500 if any error occurred.

Sample Request

HTTP Header

```
DELETE http://130.206.118.4:8080/cipa-smp-full-webapp/iso6523-actorid-
upis::0088:5798000000112/services/busdox-docid-
qns::urn:oasis:names:specification:ubl:schema:xsd:Invoice-
```

```
12::Invoice%23%23urn:www.cenbii.eu:transaction:biicoretrdm010:ver1.0:%23urn:www.peppol.eu:b
is:peppol4a:ver1.0::2.0 HTTP/1.1
Accept-Encoding: gzip,deflate
Authorization: Basic dGVzdGVyOnRlc3Q=
Host: 130.206.118.4:8080
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
```

Text

N/A

Sample Response

HTTP header

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Pragma: No-cache
Expires: Thu, 01 Jan 1970 01:00:00 CET
Content-Length: 0
Date: Fri, 22 Jan 2016 09:47:52 GMT
Cache-Control: no-cache, proxy-revalidate
Connection: Keep-Alive
```

Text

N/A

Error codes

HTTP code	HTTP Message	Business code	Meaning
200	OK	n/a	The request was completed successfully
400	Bad Request	OTHER_ERROR	Some other specific error was encountered processing the request (more information in the ErrorDescription field)
401	Unauthorized	UNAUTHORIZED	The user is not granted the right to issue this request
404	Resource not found	NOT_FOUND	The requested information was not found
500	Internal Server Error	TECHNICAL	Some unexpected technical error occurred (detailed information is available in the response)

Table 7 – UC05 Error codes

Audit

The following information must be audited for this service (more details under §2.6.5 – 'Auditing'):

- AdministratorIdentifier
- AccessTime
- Operation
- ParticipantIdentifier
- ParticipantIdentifierScheme
- DocumentIdentifier
- DocumentIdentifierScheme
- IpAddress
- RequestHeader
- ResponseHeader

- HTTP code
- Business code
- ErrorDescription

2.5. Information retrieval use cases

The following use cases are mainly intended for the sender participants' type of users in order for them to collect information on the target receivers. They are based on the 'standard' OASIS XSD (cf. §3.1.1 – "Original official OASIS SMP XSD").

2.5.1. UC06 - Retrieve Service Group

2.5.1.1. Use case

Brief description

Obtain the list of services provided by a specific receiver participant (collection of references to the ServiceMetaData's).

This service provides the information related to the Service Group according to the input duplet participantIdentifier+participantIdentifierScheme.

Returns information from the ServiceMetadata table only (references to actual MetaData) (Cf. [REF7] §2.1). A sender (ed. "user") may want to discover what document types can be handled by a specific participant identifier.

Such discovery is relevant for applications supporting several equivalent business processes.

This is enabled by a pattern where the sender first retrieves the ServiceGroup entity, which holds a list of references to the ServiceMetadata resources associated with it.

The ServiceMetadata in turn holds the metadata information that describes the capabilities associated with the recipient participant identifier.

Actors

User

Preconditions

The requester application has previously resolved the address of the SMP from the DNS.

Referenced service group was previously defined by the receiver.

Basic flow event

Step

- 1 The user request one service group references to the SMP
- 2 The SMP validates the request and retrieves the information from its configuration database (into table ServiceGroup and Service Metadata tables).
- 3 The user receives the participant's service group information
- 4 Use case ends with success

Exception flows

- 1a **SMP is not reachable**
 - 1a1 The user receives a network connection error
 - 1a2 Use case ends

2a Request is not well formed (or any other business/technical error)

2a1 The SMP replies with HTTP error "400 Bad request" or "500 Internal server error" with details on the error allowing to identify the error in the request (cf. "Error codes" table below)

2a2 The receiver receives the error message

2a3 Use case ends

2b ServiceGroup is not defined

2b1 The SMP replies with HTTP error "404 Resource not found"

2b2 The receiver receives the error message

2b3 Use case ends

Post conditions**Successful conditions**

The user receives ServiceGroup information for the requested receiver participant.

Failure conditions

The user received no ServiceGroup information about the requested receiver participant.

2.5.1.2. REST Service: GetServiceGroup

Input: ParticipantIdentifier

Represents the business level endpoint key and key type, e.g., a DUNS or GLN number that is associated with a group of services. See the ParticipantIdentifier section of the 'Common Definitions' document [BDEN-CDEF] for information on this data type.

Execution:

Selects all service Metadata related to the ServiceGroup specified by the provided ParticipantIdentifier and build the corresponding URI from it.

NB: there is no interaction with the SML (from the SMP).

Output: ServiceGroup

This SMP service will return the reference URI for the user that will enable him to retrieve all information about the services that a participant (receiver) participates in, i.e., all service metadata of the specified participant. To obtain the details on those services, the ServiceMetadata can be obtained from the SMP using the references provided.

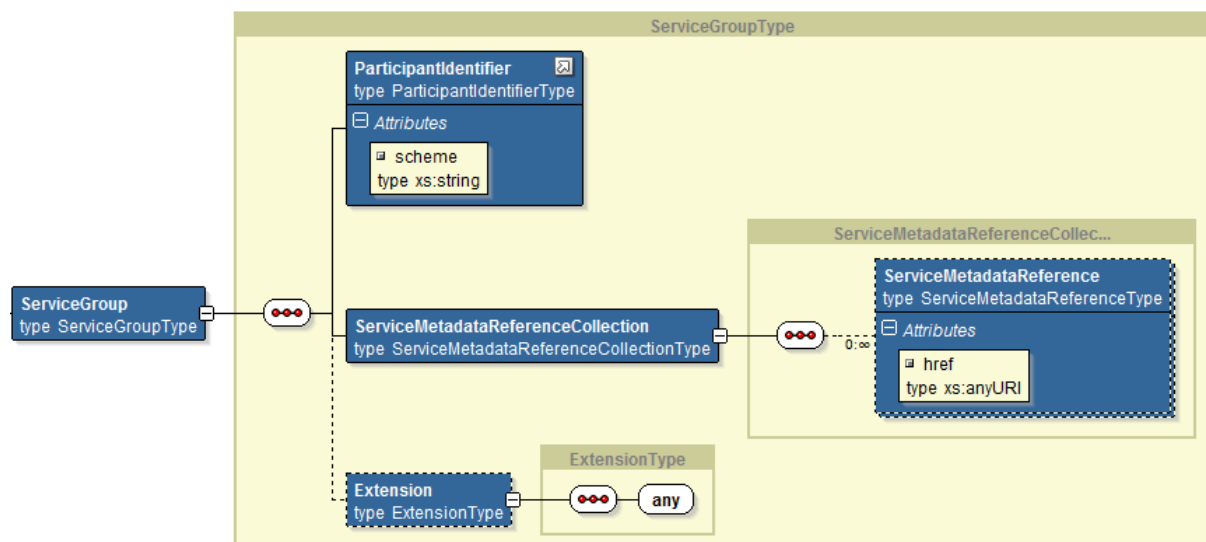


Figure 8- ServiceGroup data model

Sample Request

HTTP Header

```
GET http://130.206.118.4:8080/cipa-smp-full-webapp/iso6523-actorid-upis::0088:5798000000112 HTTP/1.1
Accept-Encoding: gzip,deflate
Host: 130.206.118.4:8080
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
```

Text

N/A

Sample Response

HTTP header

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/xml
Content-Length: 959
Date: Thu, 21 Jan 2016 08:38:33 GMT
Cache-Control: proxy-revalidate
Connection: Keep-Alive
```


Text

```

<ServiceGroup xmlns="http://docs.oasis-open.org/bdxr/ns/SMP/2016/05 ">
  <ParticipantIdentifier scheme="busdox-actorid-upis">
    0010:5798000000001
  </ParticipantIdentifier>
  <ServiceMetadataReferenceCollection>
    <ServiceMetadataReference href="http://serviceMetadata.eu/busdox-actorid-upis%3A%3A0010%3A5798000000001/services/bdx-
docid-qns%3A%3Aurn%3Aaasis%3Anames%3Aspecification%3Aubl%3Aschema%3Axsd%3Ainvoice-2%3A%3Ainvoice%23%23UBL-2.0" />
  </ServiceMetadataReferenceCollection>
  <Extension>
    <ex:Test xmlns:ex="http://test.eu">Test</ex:Test>
  </Extension>
</ServiceGroup>

```

Error codes

HTTP code	HTTP Message	Business code	Meaning
200	OK	n/a	The request was completed successfully
400	Bad Request	OTHER_ERROR	Some other specific error was encountered processing the request (more information in the ErrorDescription field)
404	Resource not found	NOT_FOUND	The requested information was not found
500	Internal Server Error	TECHNICAL	Some unexpected technical error occurred (detailed information is available in the response)

Table 8 – UC06 Error codes

Audit

The following information must be audited for this service (more details under §2.6.5 – 'Auditing'):

- AccessTime
- Operation
- ParticipantIdentifier
- ParticipantIdentifierScheme
- IpAddress
- RequestHeader
- ResponseHeader
- ResponseText
- HTTP code

2.5.2. UC07 - Retrieve Service Metadata

2.5.2.1. Use case

Brief description

Obtain detailed definition about one specific service of a specific participant for all supported transport. This service retrieves the SignedServiceMetadata according to the input quadruplet participantIdentifier+participantIdentifierScheme+documentIdentifier+documentIdentifierScheme. Returns information from the Endpoint table.

Actors

User

Preconditions

The user application has previously resolved the address of the SMP from the DNS. Referenced service group and required Service Meta data were previously defined by the receiver.

Basic flow event

Step

- 1 The user requests the detailed information of a receiver's service to the SMP
- 2 The SMP validates the request, retrieves the information from its configuration database and sends its as response to the user
- 3 The user receives the participant's service detailed information
- 4 Use case ends with success

Alternative flows

3a **Redirect**

3a1

The configuration refers to another SMP. The SMP returns the redirection information to the user

3a2

The user reinitiates the same request to that other SMP: restart use case at step 1

3a3

Use case ends

Exception flows

1a **SMP is not reachable**

1a1

The user receives a network connection error

1a2

Use case ends

2a **Request is not well formed (or any other business/technical error)**

2a1

The SMP replies with HTTP error "400 Bad request" or "500 Internal server error" with details on the error allowing to identify the error in the request (cf. "Error codes" table below)

2a2

The receiver receives the error message

2a3

Use case ends

2b **ServiceGroup or ServiceMetadata is not defined**

2b1

The SMP replies with HTTP error "404 Resource not found"

2b2 The receiver receives the error message

2b3 Use case ends

2a2a **Multiple redirect**

2a2a1 The client receives redirect information for the 2nd time (and must ignore it)

2a2a2 Use case ends

Post conditions

Successful conditions

The user receives ServiceMetaData information for the requested receiver participant.

Failure conditions

The user received no Metadata information about the requested receiver participant.

2.5.2.2. REST Service: GetSignedServiceMetadata

Input: *ServiceMetadataReference*; i.e., the PK made of 4 fields that uniquely identify the ServiceMetadata entry in the SMP configuration.

Execution:

This service will return necessary information for the user to send documents to the receiver, this information is held in the *ServiceInformation* structure, i.e., the information stored in tables Process and Endpoint (related to the requested service metadata and highlighted into red squares below):

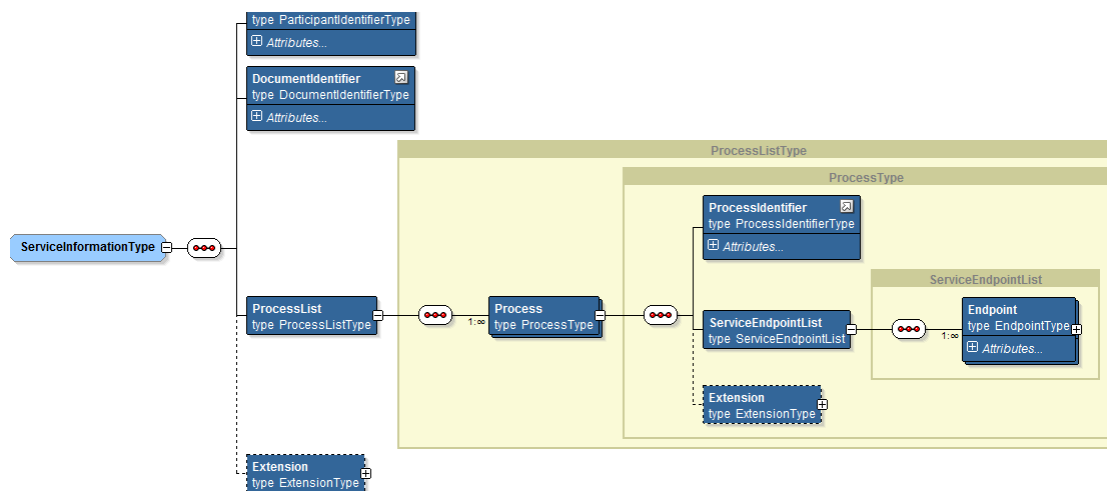


Figure 9- ServiceInformation data model

NB: there is no interaction with the SML.

Output: *SignedServiceMetadata*

Cf. [REF7], §4.3: this data structure represents Metadata about a specific electronic service. The role of the ServiceMetadata structure is to associate a participant identifier with the ability to receive a specific document type over a specific transport. It also describes which business processes a document can participate in, and various operational data such as service activation and expiration times. The ServiceMetadata resource contains all the metadata about a service that a user Access Point needs to know in order to send a message to that service.

The SignedServiceMetadata structure holds both a *ServiceMetadata* structure and the corresponding signature by the SMP to allow the user (or any other user) verifying the authenticity of the information provided by the SMP by using the public key of the SMP before sending any document to the receiver.

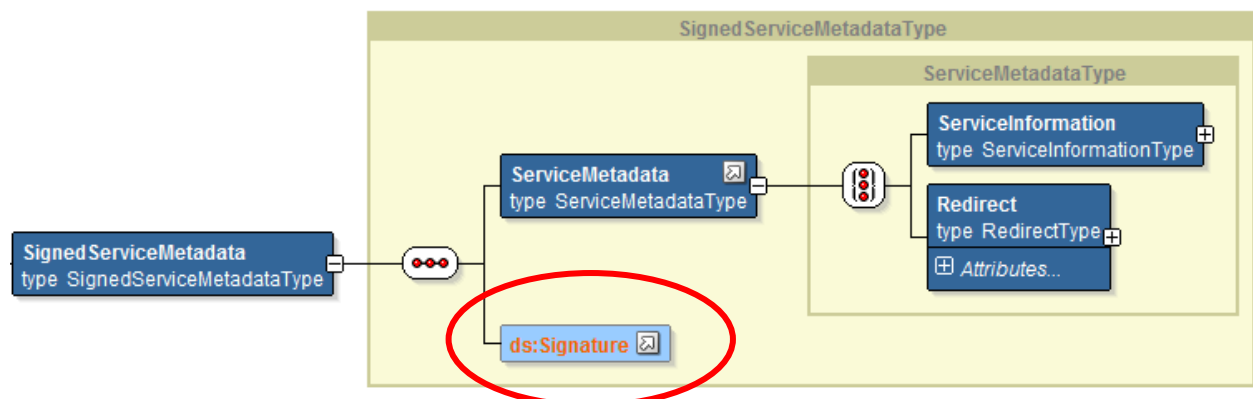


Figure 10- SignedServiceMetadata data model

Output (alternative): Redirection (supports the alternative flow 'a' in the use case)

Eventually, this service will return *redirect* information instead of the *ServiceInformation* information itself, when it is held by another SMP.

Redirection is exhaustively explained in [REF7] §4.3 ServiceMetadata and in [REF4] §2.1.3 Service Metadata Publisher Redirection.

In such a case, the information returned is the reference to the SMP that holds the corresponding "ServiceMetadata"; i.e., in the "Redirect" structure containing the target URI.

The queried SMP has in fact no information about the participant services (there is no related Process entry for that participant), instead, he has the target URI of the other SMP in the 'Redirect' column of the ServiceMetadata row for that receiver.

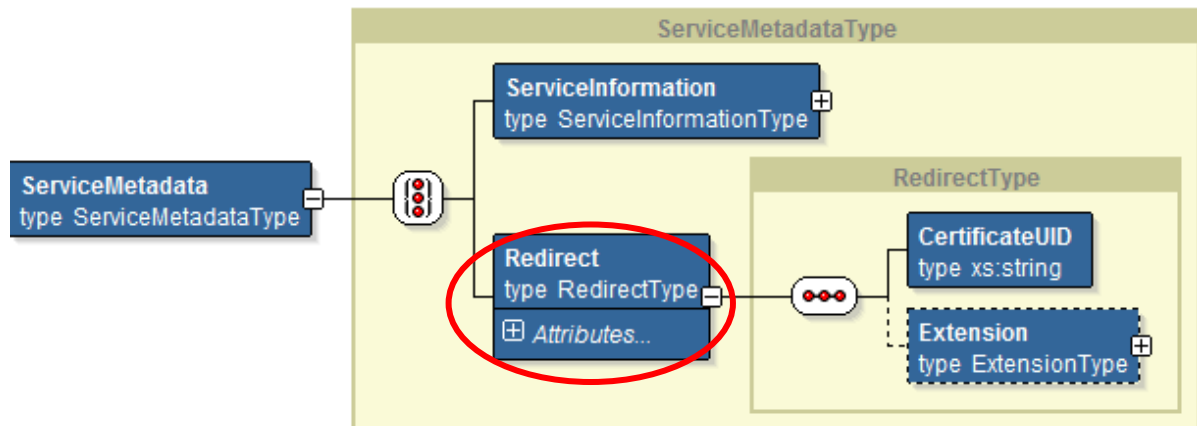


Figure 11- ServiceMetadata data model

Sample Request

HTTP Header

```

GET http://130.206.118.4:8080/cipa-smp-full-webapp/iso6523-actorid-upis::0088:5798000000112/services/busdox-docid-qns::urn:oasis:names:specification:ubl:schema:xsd:Invoice-12::Invoice%23%23urn:www.cenbii.eu:transaction:biicoretrdm010:ver1.0:%23urn:www.peppol.eu:bis:peppol4a:ver1.0::2.0 HTTP/1.1
Accept-Encoding: gzip,deflate
Host: 130.206.118.4:8080
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
  
```

Text

N/A

Sample Response

HTTP header

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/xml
Transfer-Encoding: chunked
Date: Thu, 21 Jan 2016 10:22:38 GMT
Cache-Control: proxy-revalidate
Connection: Keep-Alive
  
```

Text

```

<SignedServiceMetadata xmlns="http://docs.oasis-open.org/bdxx/ns/SMP/2016/05 ">
  <ServiceMetadata
    xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    <ServiceInformation>
      <ParticipantIdentifier scheme="busdox-actorid-upis">
        0010:57980000000001
      </ParticipantIdentifier>
      <DocumentIdentifier scheme="bdx-docid-qns">
        urn:oasis:names:specification:ubl:schema:xsd:Invoice-2::Invoice##UBL-2.02
      </DocumentIdentifier>
      <ProcessList>
        <Process>
  
```

```

<ProcessIdentifier scheme="cenbii-procid-ubl">BII04
</ProcessIdentifier>
<ServiceEndpointList>
  <Endpoint transportProfile="busdox-transport-start">
    <EndpointURI>http://busdox.org/sampleService/</EndpointURI>
    <RequireBusinessLevelSignature>>false
    </RequireBusinessLevelSignature>
    <MinimumAuthenticationLevel>2</MinimumAuthenticationLevel>
    <ServiceActivationDate>2009-05-01T09:00:00
    </ServiceActivationDate>
    <ServiceExpirationDate>2016-05-01T09:00:00
    </ServiceExpirationDate>
    <Certificate>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</Certificate>
    <ServiceDescription>invoice service</ServiceDescription>
    <TechnicalContactUrl>https://example.com
    </TechnicalContactUrl>
    <TechnicalInformationUrl>http://example.com/info
    </TechnicalInformationUrl>
  </Endpoint>
</ServiceEndpointList>
</Process>
<Process>
  <ProcessIdentifier scheme="cenbii-procid-ubl">BII07
  </ProcessIdentifier>
  <ServiceEndpointList>
    <Endpoint transportProfile="busdox-transport-start">
      <EndpointURI>http://busdox.org/sampleService/</EndpointURI>
      <RequireBusinessLevelSignature>>true
      </RequireBusinessLevelSignature>
      <MinimumAuthenticationLevel>1</MinimumAuthenticationLevel>
      <ServiceActivationDate>2009-05-01T09:00:00
      </ServiceActivationDate>
      <ServiceExpirationDate>2016-05-01T09:00:00
      </ServiceExpirationDate>
      <Certificate>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</Certificate>
      <ServiceDescription>invoice service</ServiceDescription>
      <TechnicalContactUrl>https://example.com
      </TechnicalContactUrl>
      <TechnicalInformationUrl>http://example.com/info
      </TechnicalInformationUrl>
      <Extension>
        <ex:Test xmlns:ex="http://test.eu">Test</ex:Test>
      </Extension>
    </Endpoint>
  </ServiceEndpointList>
  <Extension>
    <ex:Test xmlns:ex="http://test.eu">Test</ex:Test>
  </Extension>
</Process>
</ProcessList>
<Extension>
  <ex:Test xmlns:ex="http://test.eu">Test</ex:Test>
</Extension>
</ServiceInformation>
</ServiceMetadata>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>6r3W426Gx5foBPtasSdIEj6JvAY=</DigestValue>
    </Reference>
  </SignedInfo>

  <SignatureValue>2NJB0Pv3ORL+EpPYLCl/InXI+mDbUsV8CrWzRVJvEJMnyul2bPMe6k4MJwp9A4bTkzjvkMPARYAhyVNm6MNNIJRAFL4qdd
  sRrWa4Jgf/QF0zQgpJ7ZUPdVQ8L8A54FiPZWItOlgZCfO7sDbEcB00V4gKrmzVPBsVu6BIBOWs/UY=</SignatureValue>
  <KeyInfo>
    <X509Data>

<X509SubjectName>1.2.840.113549.1.9.1=#160e73656e64657240746573742e6265,CN=senderCN,OU=B4,O=DIGIT,L=Brussels,ST=BE,C=B
E</X509SubjectName>

```

```
<X509Certificate>MIICpTCCAg6gAwIBAgIBATANBgkqhkiG9w0BAQUFADB4MQswCQYDVQQGEwJCRTElMAkGA1UECAwCQkUxETAPBgNVBAcMCEJydXNzZWxzMQ4wDAYDVQQKDAVESUdJVDZELMAkGA1UECwwCQjQxZDZANBgNVBAMMBnJvb3RDTjEhMBkGCsGSIb3DQEQJARYMcm9vdEBOZXRhZG9wYyUwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANxLUPjIn7R0CsHf86klwNzCu+6AdmWM8fBLUHL+VXT6ayr1kkgGbfMb/vUUX6a46jRCIZBM+9IK1Hpgj9QX/QiQiWtvD+yDr6jUxahZ/w13kqFG/K81IVu9DwLBoiNwDvQ6lUbvMvV+1nWy3gjRcKIFs/C+E2uybgJxSM/sMkbAgMBAAGjOzA5MB8GA1UdIwQYMBaAFHCVSh4WnWR8MGBGedr+bJH96tc4MAkGA1UdEwQCAAwCwYDVROPBQAQDAGT wMA0GCSqGSIb3DQEQBBQUAA4GBAK6idNRxyeBmqPoSKxq7Ck3ej6R2QPpyWbwz+6/S7iCRt8PfgOu++Yu5YEjLUX1hklbQKF/JuKTLqxNnKIE6Ef65+JP2ZaI9O2wdzpRclAhAd00XbNKpyipr4jMdWmu2U8vyBBwn/utG1ZrLhAUiqPvmaQrResiGHM2xzCmVwtw</X509Certificate>
  </X509Data>
  </KeyInfo>
  </Signature>

</SignedServiceMetadata>
```

Sample Response (redirect alternative)

HTTP header

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/xml
Transfer-Encoding: chunked
Date: Thu, 21 Jan 2016 10:22:38 GMT
Cache-Control: proxy-revalidate
Connection: Keep-Alive
```

Text

```
<?xml version="1.0" encoding="utf-8" ?>

<SignedServiceMetadata xmlns="http://docs.oasis-open.org/bdxc/ns/SMP/2016/05">

  <ServiceMetadata>
    <Redirect
      href="http://serviceMetadata2.eu/busdox-actorid-upis%3A%3A0010%3A579800000001/services/bdx-docid-
qns%3A%3Aurn%3Aaosis%3Anames%3Aspecification%3Aubl%3Aschema%3Axsd%3AInvoice-2%3A%3AInvoice%23%23UBL-2.0">
      <CertificateUID>PID:9208-2001-3-279815395</CertificateUID>
    <Extension>
      <ex:Test xmlns:ex="http://test.eu">Test</ex:Test>
    </Extension>
  </Redirect>
</ServiceMetadata>

  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>6r3W426Gx5foBPtasSdIej6JvAY=</DigestValue>
      </Reference>
    </SignedInfo>

    <SignatureValue>2NJB0Pv3ORL+EpPYLCl/InXI+mDbUsV8CrWzRVJvEJMnyul2bPMe6k4MJwp9A4bTkzjvKMPARYAhyVNm6MNNIJRAFL
4qdsRrWa4Jgf/QF0zQgpJ7ZUPdVQ8L8A54FiPZWltoIlgZCf07sDbEcB00V4gKzVPBsVu6BIBOws/UY=</SignatureValue>
  <KeyInfo>
    <X509Data>

    <X509SubjectName>1.2.840.113549.1.9.1=#160e73656e64657240746573742e6265,CN=senderCN,OU=B4,O=DIGIT,L=Brussels,ST=BE
,C=BE</X509SubjectName>

  <X509Certificate>MIICpTCCAg6gAwIBAgIBATANBgkqhkiG9w0BAQUFADB4MQswCQYDVQQGEwJCRTElMAkGA1UECAwCQkUxETAPBgNVBAcMCEJydXNzZWxzMQ4wDAYDVQQKDAVESUdJVDZELMAkGA1UECwwCQjQxZDZANBgNVBAMMBnJvb3RDTjEhMBkGCsGSIb3DQEQJARYMcm9vdEBOZXRhZG9wYyUwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANxLUPjIn7R0CsHf86klwNzCu+6AdmWM8fBLUHL+VXT6ayr1kkgGbfMb/vUUX6a46jRCIZBM+9IK1Hpgj9QX/QiQiWtvD+yDr6jUxahZ/w13kqFG/K81IVu9DwLBoiNwDvQ6lUbvMvV+1nWy3gjRcKIFs/C+E2uybgJxSM/sMkbAgMBAAGjOzA5MB8GA1UdIwQYMBaAFHCVSh4WnWR8MGBGedr+bJH96tc4MAkGA1UdEwQCAAwCwYDVROPBQAQDAGT wMA0GCSqGSIb3DQEQBBQUAA4GBAK6idNRxyeBmqPoSKxq7Ck3ej6R2QPpyWbwz+6/S7iCRt8PfgOu++Yu5YEjLUX1hklbQKF/JuKTLqxNnKIE6Ef65+JP2ZaI9O2wdzpRclAhAd00XbNKpyipr4jMdWmu2U8vyBBwn/utG1ZrLhAUiqPvmaQrResiGHM2xzCmVwtw</X509Certificate>
```

```

fgOu++Yu5YEjLUX1hIkbQKF/JuKTLqxNnKIE6Ef65+JP2ZaI9O2wdzpRclAhAd00XbNKpyipr4jMdWmu2U8vyBBwn/utG1ZrLhAUiqnPvmaQr
ResiGHM2xzCmVwtse</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</SignedServiceMetadata>

```

Error codes

HTTP code	HTTP Message	Business code	Meaning
200	OK	n/a	The request was completed successfully
400	Bad Request	OTHER_ERROR	Some other specific error was encountered processing the request (more information in the ErrorDescription field)
404	Resource not found	NOT_FOUND	The requested information was not found
500	Internal Server Error	TECHNICAL	Some unexpected technical error occurred (detailed information is available in the response)

Table 9 – UC07 Error codes

Audit

The following information must be audited for this service (more details under §2.6.5 – 'Auditing'):

- AccessTime
- Operation
- ParticipantIdentifier
- ParticipantIdentifierScheme
- DocumentIdentifier
- DocumentIdentifierScheme
- IpAddress
- RequestHeader
- ResponseHeader
- ResponseText
- HTTP code

2.6. Security

2.6.1. User management

2.6.1.1. Administration process

As described in §2.3.1 – “Actors”, there are 3 types of users accessing the SMP. Among them, only “Resource Admin” and “Group Admin” types of users are registered into the configuration of the SMP.

This paragraph summarizes the process for defining the users who are responsible for managing the overall configuration of SMPs.

1. Creation of a "Group Admin"

The "Domain Admin" sets existing users as an "Group Admin".

In the picture below, "System Admin b" creates one user "Group Admin " that will manage the service groups on this SMP's.

2. Creation of a remote ServiceGroup administrator (for one Participant)

This step is necessary for remote administration of ServiceGroups (if administration is local it is done by the "Group Admin" himself).

The "System Admin":

- deploys the certificates that will be used to access the SMP for a new participant's administration (if certificates are used);
- creates manually the " Resource Admin" entry in the "Administrator" table

3. Creation of the ServiceGroup (for one Participant)

The "Group Admin" accesses the SMP via http with basic authentication with the previously assigned username and password by the "System Admin".

He uses "UC02 - Create or Update Service Group" (cf. §2.4.2) to define new service groups.

When doing so, the "Group Admin" provides either:

- A "*ServiceGroup-Owner*" in the HTTP header, i.e. some pieces of the Participant's certificates that will be used to identify the " Resource Admin" user accessing the SMP for configuration purposes (mostly for distributed SMP model)
- Nothing: in that case, the basic authentication information of the "Group Admin" (in the HTTP header) will be stored as identifier and will be himself the administrator of this ServiceGroup (cf. Step 1 of UC02 - Create or Update Service Group).

Later, he can to remove that Service Group via the same access method using "UC03 - Erase Service Group" (cf. §2.4.3).

In the picture below, "Group Admin b" creates one user "Resource Admin D, E, F" that will manage parties D,E and F.

4. Creation of ServiceMetadata

The "Resource Admin" accesses the SMP using its certificate.

He defines some new services using "UC04 - Create or Update Service Metadata" (cf. §2.4.4).

Later he can remove deprecated services similarly with "UC05 - Erase Service Metadata" (cf. §2.4.5).

In the picture below, "Resource Admin D, E, F" defines some of the services for one or several parties among D, E and F.

5. Discovering a participant's services capabilities

The Participant access the SMP with no authentication.

He uses "UC06 - Retrieve Service Group" (cf. §2.5.1) and "UC07 - Retrieve Service Metadata" (cf. §2.5.2) to collect eDelivery information on another participant he wants to exchange messages with.

In the picture below, "Participant C" collects metadata from one (and only one) participant among D, E and F.

The following diagram illustrates distributed (remote) "Resource Admin"'s:

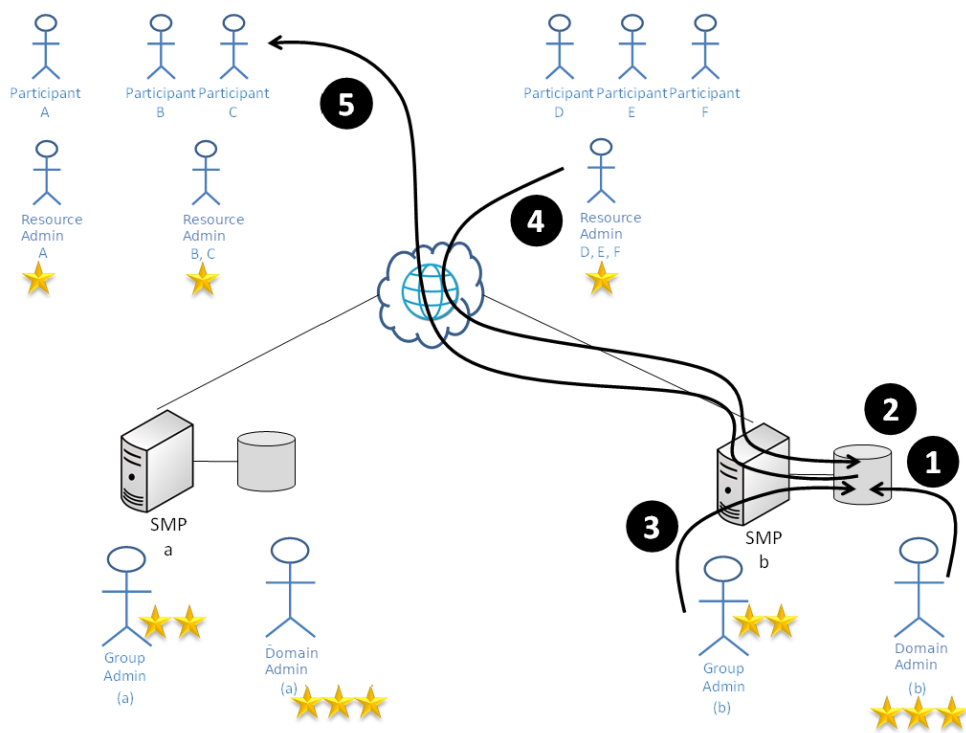


Figure 12- Remote administration model

The following diagram illustrates centralised ServiceGroup management (by the "Group Admin"):

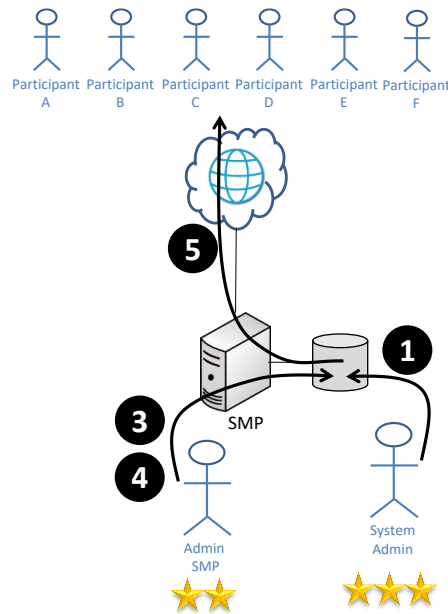


Figure 13- Local administration model

The specifications allow the coexistence of both models: some domain may decide to manage some ServiceGroups centrally (by the "Group Admin"), others in a distributed manner (by multiple remote "Resource Admin" 's).

2.6.1.2. Simple User

The regular users (Actor "User") are any user accessing the system public services. As these users do not need to be authenticated, they do not have to be known in advance by the System and are therefore not preregistered in any way on the SMP.

2.6.1.3. System Admin

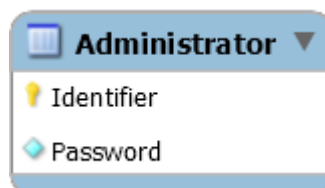
The "System Admin" actor is, as the name suggests, a system user having special accesses to the system. In the purpose of user administration for the SMP, this "system user" is able to modify the content of the SMP configuration database, i.e. he must have full read/write data access on this configuration database, in particular table "Administrator" described in §2.6.1.4 "Security tables".

He is responsible for creating and maintaining the definition of all "Group Admin" and "Resource Admin" administrators (as described by use case UC01).

2.6.1.4. Security tables

2.6.1.4.1. Administrator

This table identifies the **administrators** of the SMP; i.e. "Group Admin" and "Resource Admin" actors introduced above.



There are two possible means to obtain access to the SMP non-public services:

- through **basic authentication**; i.e. with a simple **username/password** authentication method:

- **Identifier** column contains then the username used to identify the administrator at logon
 - **Password** column contains then the hash of the password used to authenticate the user at logon
- thru **two-way SSL** using PKI infrastructure (i.e., X.509 certificates):
 - the **Identifier** column contains pieces of the client certificate that are forwarded by the reverse proxy in the http header to the server (cf. 2.6.3 – “HTTP Authentication”)
 - **Password** column is unused for 2-way-ssl since the certificate is not validated by the application layer itself; the prerequisite being that the user’s certificate is already present in the truststore of the reverse proxy server.

In all cases, it is the responsibility of the SMP to hash the password (and apply the same algorithm for authentication). The participant will send the password in 'clear' in the HTTP header.

2.6.1.4.2. Ownership (of service group)

1-N relationship materialization between the service groups and the “Resource Admin” type of users of the SMP. More details are available under §2.6.1.6 – “Resource Resource Admin”.

This relationship allows the system to identify which ‘user’ (singular) is allowed to modify(/delete) all the information related to all the ServiceMetadata of one given ‘ServiceGroup’.

2.6.1.5. Group Admin

The “Group Admin” user is created by the system administrator (cf. §2.3.1 – “Actors” and §2.4.1 – “UC01 - Manage Administrators”).

Some information in the system (not detailed here) allows the system to identify this specificity of such users.

2.6.1.6. Resource Admin

The “Resource Admin” user of one specific participant will be allowed to use all the services that modify the definition of the ServiceGroups, i.e. to create, modify or delete SignedServiceMetadata belonging to/referenced by a ServiceGroup.

To allow the access right verification, the configuration holds a link between the “Resource Admin” and the related ServiceGroup via an “ownership relationship” materialized as shown here in the configuration:

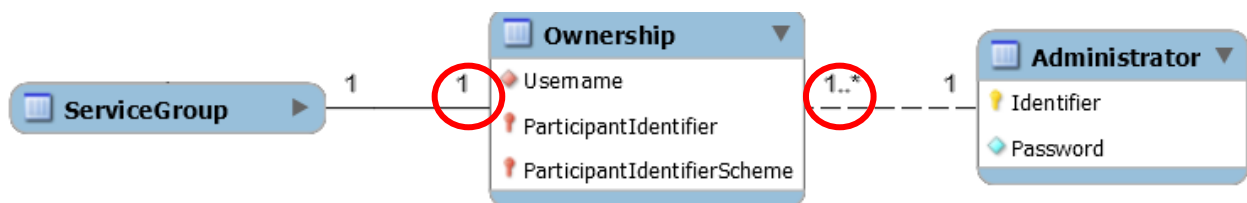


Figure 14- ServiceGroup ownership

The ServiceGroup can be managed by:

- The related "Resource Admin" (if any); and,
- The Group Admin (who may administer all service groups).

This **link** is established when the ServiceGroup is created (or updated).

2.6.2. [Access rights](#)

The following matrix clarifies the access rights of each actor to all use cases and the type of authentication method that are supported for each user role:

	System Admin	Group Admin	Resource Admin	User
UC01 Manage Administrators	X			
UC02 Create or Update Service Group		X		
UC03 Erase Service Group		X		
UC04 Create or Update Service Metadata		X	X	
UC05 Erase Service Metadata		X	X	
UC06 Retrieve Service Group	X	X	X	X
UC07 Retrieve Service Metadata	X	X	X	X

Authentication method (Acceptance and Production at EC)

System + database authentication	X			
HTTP Basic authentication		X	-	
HTTP 2-way-ssl			X	
None				X

Authentication method (Test at EC)

System + database authentication	X			
HTTP Basic authentication		X	X	
HTTP 2-way-ssl			-	
None				X

Table 10 – Access rights summary

NB: attention, "Group Admin" user may act on behalf of all the "Resource Admin" defined in the SMP.

2.6.3. [HTTP Authentication](#)

SSL will be used at all times (i.e., for any exchange of message between a SMP and any participant, acting as a sender or as a receiver.) to guarantee the validity of the information provided by the SMP to the sender and receiver.

Two authentication methods are supported and vary with services and/or user's roles:

1. Basic HTTP authentication (username/password) – for "Group Admin" users and optionally for "Resource Admin" users (cf. "Test at EC" above).
2. HTTP 2-way SSL for remote "Resource Admin" users (only) when and if this method is preferred for those to basic authentication (see "Authentication method" tables in §2.6.2 above: this authentication method might be used at EC in production environment).

If HTTP basic authentication is available for both types of users, 2-way SSL will also be usable for authenticating "Resource Admin" users. In order to achieve this, all the PUT and DELETE services on ServiceMetadata data type (cf. UC04 and UC05) will be able to use that type of authentication.

In order to provide this possibility, the certificates of the authorized administrators (“Resource Admin” users) will be deployed on the necessary SMPs on dedicated keystores. This will allow the transport layers to establish necessary trust without any addition to the existing message structure.

Also, the fields in *Administrator* table will be used as follows differently in the different possible cases (by user roles and authentication methods):

User role:	Group Admin	Resource Admin	
Authentication type:	Basic Authentication	2 way-ssl	Basic Authentication

Identifier:	Basic username	HTTP client cert	Basic username
Password:	password hash	n/a	password hash

Table 11 – Authentication types usage

NB: Only basic authentication is allowed for “Group Admin” user since they are intended to be “intranet” users rather than “internet” ones.

The password field, when applicable, will hold a hash value of the password.

2.6.4. Reverse proxy

This paragraph discusses the specific deployment in production and at the European Commission for information only.

An existing BDMSL server is already hosted at the European Commission behind a “Reverse Proxy” as explained in [REF10] §11.2.2 “Reverse proxy with SSL”. In this case, 2-way SSL is set up on the reverse proxy and the application server hosting the application can use the HTTP protocol.

A similar configuration could be used at the European Commission for SMP’s where 2-way SSL must be used.

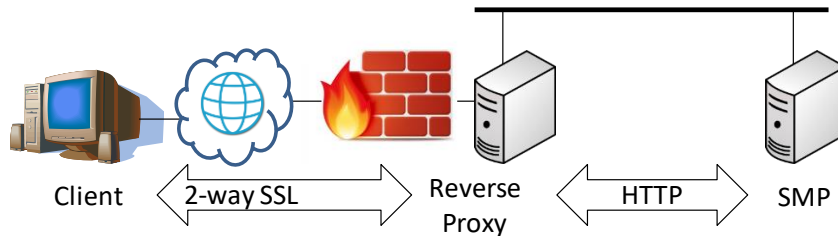


Figure 15- Reverse proxy at EC

As stated above, this type of access will be provided for remote “Resource Admin” type of users only and is optional. Basic authentication will be used instead when there is no remote “Resource Admin”; i.e., when the “Group Admin” administers the ServiceGroup himself.

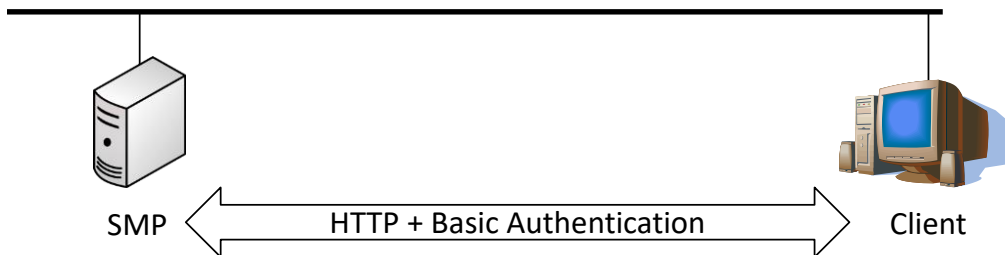


Figure 16- Basic authentication

Therefore, the authentication mechanism for services modifying Service Metadata will behave as follow:

- Search HTTP header for “Client Certificate” data (conversion performed by the reverse proxy). If present, use these to authenticate user against the “username” present in table “Administrator”.

The “Client Certificate” values will be inserted in the HTTP header to the SMP by the Reverse Proxy out of the X.509 Certificate.

The X.509 attributes to be used will be defined in the detailed design.

The value stored in the “Administrator” table column “username” should contain necessary information to validate that the provided value match.

- If no “Client certificate” information is available (meaning there is no reverse proxy between the client and the SMP), use Basic HTTP authentication: check provided username and password (clear value) to identify and authenticate the requesting user and authorize access.

To summarize, the SMP deployed at the European Commission has the following accesses:

1. Direct System & database logins are used by the System Admin.
2. Basic authentication over HTTP is used for the Group Admin and Resource's that are on the same local network than the SMP itself.
SMP authenticates local Group Admin's based on the hash of the password that was stored by the System admin.
3. Certificates of remote "Admin Service Group's" are authenticated by the Reverse Proxy.
4. Information of the client's certificate is provided to the SMP for authorization (*Client-Cert attribute*) – password is blank
5. Parties do not have to authenticate themselves but may use the SMP's certificate to authenticate it.

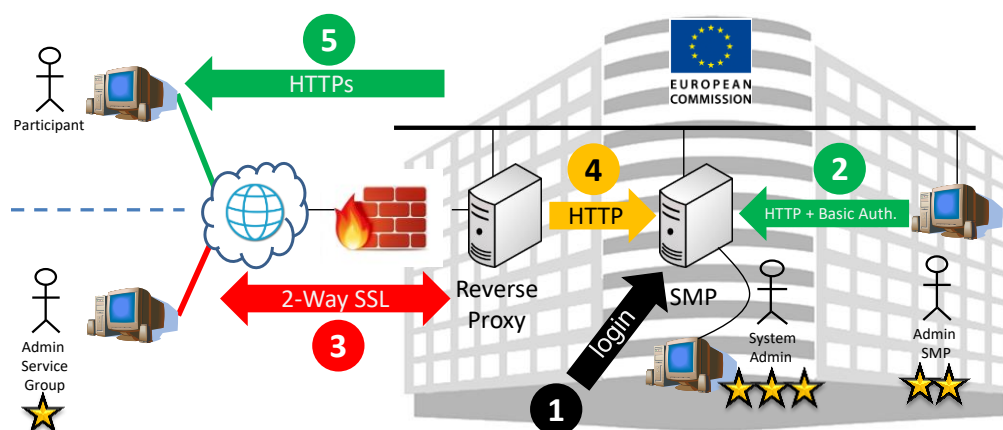


Figure 17- Overall administration model

2.6.5. Auditing

All SMP services will log relevant information regarding the access as specified in the table below:

Column	Description	Manage Administrators	Create or Update Service Group	Erase Service Group	Create or Update Service Metadata	Erase Service Metadata	Retrieve Service Group	Retrieve Service Metadata
		UC01	UC02	UC03	UC04	UC05	UC06	UC07
AdministratorIdentifier	Whom the request was initiated from	n/a	X	X	X	X	-	-
AccessTime	When the access was made	n/a	X	X	X	X	X	X
Operation	What was performed (servicename)	n/a	X	X	X	X	X	X
ParticipantIdentifier	The identifier of the participant	n/a	X	X	X	X	X	X
ParticipantIdentifierScheme	The scheme of the identifier of the participant	n/a	X	X	X	X	X	X
DocumentIdentifier	The identifier of the document	n/a	-	-	X	X	-	X
DocumentIdentifierScheme	The scheme of the identifier of the document	n/a	-	-	X	X	-	X
IpAddress	The source IP address from which the request was initiated	n/a	X	X	X	X	X	X
RequestHeader	The HTTP Header of the request	n/a	X	X	X	X	X	X
RequestText	The text of the request (XML)	n/a	X	-	X	-	-	-
ResponseHeader	The HTTP Header of the response	n/a	X	X	X	X	X	X
ResponseText	The text of the response (XML)	n/a	-	-	-	-	X	X
HTTP code	The HTTP response code	n/a	X	X	X	X	X	X
Business code	The application-level error code for HTTP error 40x	n/a	X	X	X	X	-	-
ErrorDescription	The description of the error (free text)	n/a	X	X	X	X	-	-

Table 12 – Audited information by use case

It will be a design decision to save this auditing information either in a database table, log files or any type of persistence solution provided that the information is saved and is searchable.

Audited information must be kept accessible (online or offline) during at least 3 months.

No hard link (with foreign keys) will be established between this table and the User or the participant identifier one to allow:

- Keeping the logs relating to one user or one participant that is later removed from the database (if ever applicable),
- Keeping track of unauthorized calls for unidentified users or erroneous participant identifications.

2.7. Special requirements

- The SMP should be available 99%.
- Response time should be less than 5s for the GET services for 90% of the requests
- Response time should be less than 10s for the PUT/DELETE services for 90% of the requests

3. ANNEX

3.1. XSD files

3.1.1. Original official OASIS SMP XSD

Reference: <http://docs.oasis-open.org/bdxx/bdx-smp/v1.0/cs03/schemas/bdx-smp-201605.xsd>

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Service Metadata Publishing (SMP) Version 1.0
  Committee Specification 03
  30 June 2016
  Copyright (c) OASIS Open 2016. All Rights Reserved.
  Source: http://docs.oasis-open.org/bdxx/bdx-smp/v1.0/cs03/schemas/
  Latest version of the specification: http://docs.oasis-open.org/bdxx/bdx-smp/v1.0/bdx-smp-v1.0.html
  TC IPR Statement: https://www.oasis-open.org/committees/bdxx/ipr.php
-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://docs.oasis-
open.org/bdxx/ns/SMP/2016/05" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
elementFormDefault="qualified" targetNamespace="http://docs.oasis-open.org/bdxx/ns/SMP/2016/05"
id="ServiceMetadataPublishing">
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
  <xs:element name="ServiceGroup" type="ServiceGroupType"/>
  <xs:element name="ServiceMetadata" type="ServiceMetadataType"/>
  <xs:element name="SignedServiceMetadata" type="SignedServiceMetadataType"/>
  <xs:complexType name="SignedServiceMetadataType">
    <xs:sequence>
      <xs:element ref="ServiceMetadata"/>
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="ServiceMetadataType">
    <xs:choice>
      <xs:element name="ServiceInformation" type="ServiceInformationType"/>
      <xs:element name="Redirect" type="RedirectType"/>
    </xs:choice>
  </xs:complexType>
  <xs:complexType name="ServiceInformationType">
    <xs:sequence>
      <xs:element ref="ParticipantIdentifier"/>
      <xs:element ref="DocumentIdentifier"/>
      <xs:element name="ProcessList" type="ProcessListType"/>
      <xs:element name="Extension" type="ExtensionType" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="ProcessListType">
    <xs:sequence>
      <xs:element name="Process" type="ProcessType" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="ProcessType">
    <xs:sequence>
      <xs:element ref="ProcessIdentifier"/>
      <xs:element name="ServiceEndpointList" type="ServiceEndpointList"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

```

        <xs:element name="Extension" type="ExtensionType" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="ServiceEndpointList">
    <xs:sequence>
        <xs:element name="Endpoint" type="EndpointType" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="EndpointType">
    <xs:sequence>
        <xs:element name="EndpointURI" type="xs:anyURI"/>
        <xs:element name="RequireBusinessLevelSignature" type="xs:boolean" minOccurs="0"
default="false"/>
        <xs:element name="MinimumAuthenticationLevel" type="xs:string" minOccurs="0"/>
        <xs:element name="ServiceActivationDate" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="ServiceExpirationDate" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="Certificate" type="xs:base64Binary"/>
        <xs:element name="ServiceDescription" type="xs:string"/>
        <xs:element name="TechnicalContactUrl" type="xs:anyURI"/>
        <xs:element name="TechnicalInformationUrl" type="xs:anyURI" minOccurs="0"/>
        <xs:element name="Extension" type="ExtensionType" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="transportProfile" type="xs:string" use="required"/>
</xs:complexType>
<xs:complexType name="ServiceGroupType">
    <xs:sequence>
        <xs:element ref="ParticipantIdentifier"/>
        <xs:element name="ServiceMetadataReferenceCollection"
type="ServiceMetadataReferenceCollectionType"/>
        <xs:element name="Extension" type="ExtensionType" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="ServiceMetadataReferenceCollectionType">
    <xs:sequence>
        <xs:element name="ServiceMetadataReference" type="ServiceMetadataReferenceType"
minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="ServiceMetadataReferenceType">
    <xs:attribute name="href" type="xs:anyURI"/>
</xs:complexType>
<xs:complexType name="RedirectType">
    <xs:sequence>
        <xs:element name="CertificateUID" type="xs:string"/>
        <xs:element name="Extension" type="ExtensionType" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="href" type="xs:anyURI" use="required"/>
</xs:complexType>
<xs:element name="ParticipantIdentifier" type="ParticipantIdentifierType"/>
<xs:element name="DocumentIdentifier" type="DocumentIdentifierType"/>
<xs:element name="ProcessIdentifier" type="ProcessIdentifierType"/>
<xs:element name="RecipientIdentifier" type="ParticipantIdentifierType"/>
<xs:element name="SenderIdentifier" type="ParticipantIdentifierType"/>
<xs:complexType name="ParticipantIdentifierType">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="scheme" type="xs:string"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>

```

```

    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="DocumentIdentifierType">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="scheme" type="xs:string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="ProcessIdentifierType">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="scheme" type="xs:string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="ExtensionType">
  <xs:annotation>
    <xs:documentation>
      A single extension for private use.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionID" type="xs:token">
      <xs:annotation>
        <xs:documentation>
          An identifier for the Extension assigned by the creator of the extension.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionName" type="xs:string">
      <xs:annotation>
        <xs:documentation>
          A name for the Extension assigned by the creator of the extension.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionAgencyID" type="xs:string">
      <xs:annotation>
        <xs:documentation>
          An agency that maintains one or more Extensions.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionAgencyName" type="xs:string">
      <xs:annotation>
        <xs:documentation>
          The name of the agency that maintains the Extension.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionAgencyURI" type="xs:anyURI">
      <xs:annotation>
        <xs:documentation>
          A URI for the Agency that maintains the Extension.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

```
        </xs:annotation>
    </xs:element>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionVersionID"
type="xs:normalizedString">
        <xs:annotation>
            <xs:documentation>
                The version of the Extension.
            </xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionURI" type="xs:anyURI">
        <xs:annotation>
            <xs:documentation>
                A URI for the Extension.
            </xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionReasonCode" type="xs:token">
        <xs:annotation>
            <xs:documentation>
                A code for reason the Extension is being included.
            </xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element maxOccurs="1" minOccurs="0" name="ExtensionReason" type="xs:string">
        <xs:annotation>
            <xs:documentation>
                A description of the reason for the Extension.
            </xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:any namespace="##other" processContents="lax"/>
</xs:sequence>
</xs:complexType>

</xs:schema>
```

3.1.2. Extended SMP XSD

ErrorResponse used as response has been defined in order to allow returning some detailed information on the error that as occurred.

The values for elements "BusinessCode" and "ErrorDescription" are further detailed under §3.2 –"Errors codes table".

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="ec:services:SMP:1.0" targetNamespace="ec:services:SMP:1.0"
  elementFormDefault="qualified" id="ServiceMetadataPublishing">
  <xs:element name="ErrorResponse" type="ErrorResponseType"/>
  <xs:complexType name="ErrorResponseType">
    <xs:sequence>
      <xs:element name="BusinessCode" type="xs:string"/>
      <xs:element name="ErrorDescription" type="xs:string" minOccurs="0"/>
      <xs:element name="ErrorUniqueld" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

3.2. Errors codes table

The following table summarizes all possible errors returned by the SMP services:

HTTP code	HTTP Message	Business code	Meaning	Applicable UC						
				UC01	UC02	UC03	UC04	UC05	UC06	UC07
				n/a	PUT	DEL	PUT	DEL	GET	GET
200	OK	n/a	The request was completed successfully.	-	X	X	X	X	X	X
201	Created	n/a	The PUT operation completed successfully.	-	X		X		-	-
400	Bad Request	XSD_INVALID	The XML included in the request is not validate against the XSD defining the input structure.	-	X		X		-	-
400	Bad Request	MISSING_FIELD	Some field that is optional in the XSD but mandatory for this invocation is missing (missing field	-	X		X		-	-

HTTP code	HTTP Message	Business code	Meaning	Applicable UC						
				UC01	UC02	UC03	UC04	UC05	UC06	UC07
				n/a	PUT	DEL	PUT	DEL	GET	GET
			name in description).							
400	Bad Request	WRONG_FIELD	Some field is valid against XSD definition, but the more specific content is invalid (erroneous field name in description) Or Some header field is either missing or invalid.	-	X		X		-	-
400	Bad Request	OUT_OF_RANGE	Some numeric (or date field) is out of the valid range (erroneous field name in description).	-			X		-	-
400	Bad Request	UNAUTHOR_FIELD	Some field that is optional in the XSD but forbidden for this invocation is present (unauthorized field name in description).	-			X		-	-
400	Bad Request	FORMAT_ERROR	Some field is expected to have a specific format is not valid (erroneous field name in description).		X	X	X		-	-
400	Bad Request	USER_NOT_FOUND	The referenced " Resource Admin" was not found as Administrator.		X				-	-

HTTP code	HTTP Message	Business code	Meaning	Applicable UC						
				UC01	UC02	UC03	UC04	UC05	UC06	UC07
				n/a	PUT	DEL	PUT	DEL	GET	GET
400	Bad Request	OTHER_ERROR	Some other specific error was encountered processing the request (more information in the <i>ErrorDescription</i> field).				(x)	(x)	(x)	(x)
401	Unauthorized	UNAUTHORIZED	The user is not granted the right to issue this request.	-	X	X	X	X	-	-
404	Resource not found	NOT_FOUND	The requested information was not found.	-		X		X	X	X
500	Internal Server Error	TECHNICAL	Some unexpected technical error occurred (detailed information is available in the response).	-	X	X	X	X	X	X

Legend

- X = This service returns this kind of errors
- (x) = This service might return this kind of errors, and in the event might provide more unstructured information in the *errorDescription* field of the *ErrorResponse* structure.

3.3. Detailed Errors structure

In case of error, a response text will be provided, in an “ErrorResponse” type of element (cf. definition in 3.1.2 – “Extended SMP XSD ”).

The *ErrorResponse* holds the following elements:

- *BusinessCode*

This code allows the client application to behave appropriately according to the encountered error. The expected values are summarized in §3.2 –“Errors codes table” and their applicability explicitly specified for each service in the corresponding paragraph.

- *ErrorDescription*

This description provides some detailed information on the encountered error. Its content is not predefined and should be intended to help the client developer or administrator to investigate the encountered error.

- *ErrorUniqueld*

This identifier uniquely identifies the occurrence of the error. This value is intended to facilitate further investigations on a specific error in particular to search into log files.

Example:

```
<ErrorResponse xmlns="ec:services:SMP:1.0">
  <BusinessCode>TECHNICAL</BusinessCode>
  <ErrorDescription>Some unexpected technical error occurred. (detailed information available here)</ErrorDescription>
  <ErrorUniqueld>5378C627DA4275F698458AB6845C68456845</ErrorUniqueld>
</ErrorResponse>
```

4. LIST OF FIGURES

Figure 1 – eDelivery components.....	9
Figure 2 - The four corner model	10
Figure 3- Logical data model (high level view)	12
Figure 4- XSD's usage.....	Error! Bookmark not defined.
Figure 5- Use cases diagram	19
Figure 6- ServiceGroup data model.....	27
Figure 7- ServiceInformation data model	37
Figure 8- Redirect data model.....	38
Figure 9- ServiceGroup data model.....	48
Figure 10- ServiceInformation data model	52
Figure 11- SignedServiceMetadata data model	52
Figure 12- ServiceMetadata data model	53
Figure 13- Remote administration model	58
Figure 14- Local administration model.....	59
Figure 15- ServiceGroup ownership.....	60
Figure 16- Reverse proxy at EC.....	62
Figure 17- Basic authentication.....	62
Figure 18- Overall administration model	63

5. LIST OF TABLES

Table 1 - XSD elements.....	16
Table 2 – Actors.....	18
Table 3 – Use cases list.....	21
Table 4 – UC02 Error codes	30
Table 5 – UC03 Error codes	34
Table 6 – UC04 Error codes	42
Table 7 – UC05 Error codes	45
Table 8 – UC06 Error codes	49
Table 9 – UC07 Error codes	56
Table 10 – Access rights summary	61
Table 11 – Authentication types usage	62
Table 12 – Audited information by use case	64

6. CONTACT INFORMATION

eDelivery Support Team

By email: EC-EDELIVERY-SUPPORT@ec.europa.eu

Support Service: 8am to 6pm (Normal EC working Days)