MediPrima UMA v.1
Cookbook
Version 1.2

This document is provided to you free of charge by the

eHealth platform

Willebroekkaai 38 – 1000 Brussel

38, Quai de Willebroek – 1000 Bruxelles

Table of contents

Contents

To the attention of: “IT expert” willing to integrate this web service.

1. Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1.0	24/03/2018	eHealth platform	Initial version
1.1	24/06/2021	eHealth platform	WS-I Compliance & Tracing
1.2	17/01/2024	eHealth platform	deleted erroneous section on encryption

2. Introduction

2.1 Goal of the service

In the following pages, a brief outline will be given on MediPrima UMA[1]. The goal of the MediPrima UMA is to offer a service to actors in the medical sector, to exchange (send, delete and search) data with the registry of UMA attestations. This registry is belonging to SocSec[2].

2.2 Goal of the document

This document is not a development or programming guide for internal applications. Instead, it provides functional and technical information and allows an organization to integrate and use the MediPrima UMA eHealth platform service.

However, in order to interact in a smooth, homogeneous and risk controlled way with a maximum of partners, these partners must commit to comply with the requirements of specifications, data format and release processes of the eHealth platform as described in this document.

Technical and business requirements must be met in order to allow the integration and validation of the MediPrima UMA eHealth platform service in the client application.

2.3 eHealth platform document references

On the portal of the eHealth platform, you can find all the referenced documents[3]. These versions or any following versions can be used for the eHealth platform service.

ID	Title	Version	Date	Author
1	SOA – Error Guide	1.0	10/06/2021	eHealth platform
2	Request test case template	3.0	22/02/2018	eHealth platform
3	WSDL	N.A.	N.A.	eHealth platform
4	MediPrima_UMA_SSO.doc	1.00	04/12/2017	eHealth platform
5	MediPrima_UMA_pipe.doc	0.02	01/12/2017	eHealth platform

2.4 External references

ID	Title	Version	Date	Author
1	http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html		24/08/2004	Web Services Interoperability Organization

[1] *In EN : UMA (Urgent Medical Aid)*
In FR : AMU (Aide Médicale Urgente)
In NL : UMH (Urgent Medische Hulp)

[2] *In EN : Social Security (SocSec)*
In FR : Sécurité Sociale (SecSoc)
In NL : Sociale Zekerheid (SocZek)

[3] ***https://ehealth.fgov.be/ehealthplatform***

3. Support

3.1 Helpdesk eHealth platform

3.1.1 Certificates

In order to access the secured eHealth platform environment you have to obtain an eHealth platform certificate, used to identify the initiator of the request. In case you do not have one, please consult the chapter about the eHealth Certificates on the portal of the eHealth platform

- ***https://www.ehealth.fgov.be/ehealthplatform/nl/ehealth-certificaten***
- ***https://www.ehealth.fgov.be/ehealthplatform/fr/certificats-ehealth***

For technical issues regarding eHealth platform certificates

- Acceptance: ***acceptance-certificates@ehealth.fgov.be***
- Production: ***support@ehealth.fgov.be***

3.1.2 For issues in production

eHealth platform contact centre:

- Phone: 02 788 51 55 (on working days from 7 am till 8 pm)
- Mail: ***support@ehealth.fgov.be***
- *Contact Form :*
  - ***https://www.ehealth.fgov.be/ehealthplatform/nl/contact*** (Dutch)
  - ***https://www.ehealth.fgov.be/ehealthplatform/fr/contact*** (French)

3.1.3 For issues in acceptance

Integration-support@ehealth.fgov.be

3.1.4 For business issues

- regarding an existing project: the project manager in charge of the application or service
- regarding a new project or other business issues: ***info@ehealth.fgov.be***

3.2 Status

The website ***https://status.ehealth.fgov.be*** is the monitoring and information tool for the ICT functioning of the eHealth services that are partners of the Belgian eHealth system.

4. Global overview

4.1 Illustration

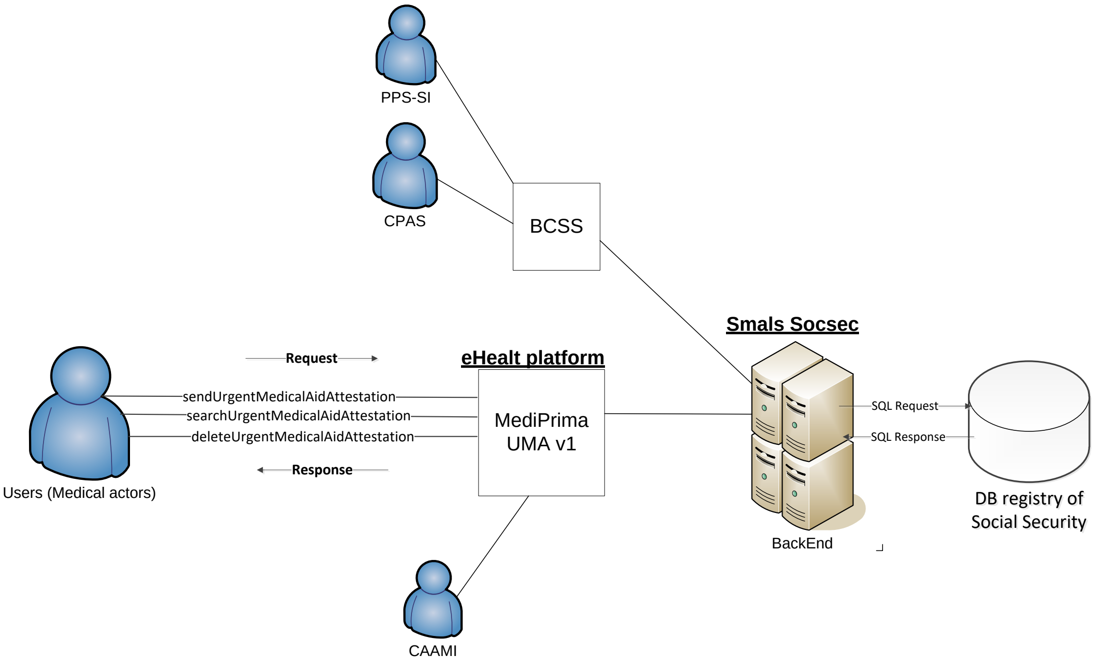


Figure 1 : Global Overview illustration

4.2 Context

The MediPrima project allows electronic management of medical aid attestations (for people in need) and billing management.

This MediPrima UMA service is created to allow exchanges of Urgent Medical Aid Attestation between medical actors and the registry of the Social security.

Category concerned:

For a person residing illegally in Belgium, the urgency of the medical aid is exclusively determined by a doctor who must then, following consultation of the patient's status in NovaPrima, produce an urgent medical aid attestation (UMAA) to received reimbursement by the State. This attestation does not contain medical data.

UMA Attestations:

Previously, care providers sent UMA attestations and invoice relating to their services to PSWC[4]. PSWC then requested reimbursement from the PPS-SI[5] and kept the paper copies (invoices and UMA attestations). PSWC had to be able to provide this attestation at the request during the inspections by the CAAMI/HZIV[6] and the inspectors of the PPS-SI.

Since Mediprima, the exchanges are done directly between a hospital/general practitioner and the CAAMI/HZIV. The CAAMI/HZIV then requests UMA attestation from the healthcare providers when the invoice is checked.

Electronic Advantages

In order to simplify the process of ex-post checks and limit the paper flow, the UMA forms are computerized and are available before invoicing.

An advantage of this computerization is that all or part of the data are available to other partners (PSWC, CAAMI/HZIV, Providers of care (doctors, pharmacists, dentists, etc.)).

A cancellation will also be possible (if the provider has created an UMA attestation by mistake).

[4] *In EN : Public Social Welfare Centre (PSWC)*
In FR : Centre public d'action sociale (CPAS)
In NL : Openbaar centrum voor maatschappelijk welzijn (OCMW)

[5] *In EN : federal Public Planning Service Social Integration (PPS-SI)*
In FR : Service fédéral de Planning Public pour l'Intégration Sociale (SPP-IS)
In NL: Programmatorische Overheidsdienst voor Maatschappelijke Integratie (POD-MI)

[6] *In FR : Caisse Auxiliaire d'Assurance Maladie Invalidité (CAAMI)*
In NL : Hulpkas voor Ziekte en Invaliditeitsverzekering (HZIV)

5. Step-by-step

5.1 Technical requirements

5.1.1 Use of the eHealth SSO solution

This section specifies how the call to STS must be done to have access to the web service (WS) . You must precise several attributes in the request.

To access to the MediPrima UMA WS, the response token must contain:

- “true” for all of the boolean certification attributes.
- A value for all the nihii11 certification attributes

If you obtain :

- obtain “false” for one boolean certification attributes
- do not obtain any value for one of the nihii11 certification attributes

contact the eHealth-Dev platform (eHealthDevSupport@ehealth.fgov.be) to verify that the requested test cases were correctly configured.

5.1.2 WS-I Basic Profile 1.1

Your request must be WS-I compliant (See external Ref). If not you will receive one of the errors SOA-03001 – SOA-03003. (See Chapter *Errors)*

5.1.2.1 Healthcare institution

5.1.2.1.1 Hospital

The SAML token request is secured with the eHealth certificate of the hospital. The certificate used by the Holder-Of-Key verification mechanism is the same eHealth certificate.

The needed attributes are the following (AttributeNamespace: "urn:be:fgov:identification-namespace"):

- The NIHII number of the hospital:
  - *urn:be:fgov:ehealth:1.0:hospital:nihii-number*
  - *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number*

Hospital must also specify which information must be asserted by eHealth:

- The NIHII number of the hospital (namespace: urn:be:fgov:identification-namespace):
  - *urn:be:fgov:ehealth:1.0:hospital:nihii-number*
  - *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number*
- To have access to Mediprima UMA, the hospital must be a recognized hospital (AttributeNamespace: urn:be:fgov:certifiednamespace:ehealth):
  - *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number:recognisedhospital:boolean*

5.1.2.1.2 OT/TD[7]

The SAML token request is secured with the eHealth certificate of the OT/TD. The certificate used by the Holder-Of-Key (HOK) verification mechanism is the same eHealth certificate.

The needed attributes are the following (AttributeNamespace: "urn:be:fgov:identification-namespace"):

- The NIHII number of the OT/TD:
  - *urn:be:fgov:ehealth:1.0:otdpharmacy:nihii-number*
  - *urn:be:fgov:ehealth:1.0:certificateholder:otdpharmacy:nihii-number*

OT/TD must also specify which information must be asserted by eHealth:

- The NIHII number of the OT/TD (namespace: urn:be:fgov:identification-namespace):
  - *urn:be:fgov:ehealth:1.0:otdpharmacy:nihii-number*
  - *urn:be:fgov:ehealth:1.0:certificateholder:otdpharmacy:nihii-number*
- To have access to Mediprima UMA, the OT/TD must be a recognized OT/TD (AttributeNamespace: urn:be:fgov:certifiednamespace:ehealth):
  - *urn:be:fgov:ehealth:1.0:certificateholder:otdpharmacy:nihii-number:recognisedotdpharmacyboolean*

5.1.2.1.3 Pharmacy

Pharmacies must specify several attributes in the request. The request to the STS is secured with the eID of the pharmacist starting the session. The certificate of the pharmacy issued by the eHealth platform is used by the HOK mechanism.

The attributes that need to be provided in the request are the following (AttributeNamespace: *urn:be:fgov:identification-namespace*):

- The social security identification number of the person starting the session (must be a pharmacist):
  - *urn:be:fgov:ehealth:1.0:certificateholder:person:ssin*
  - *urn:be:fgov:person:ssin*
- The identification of the pharmacy:
  - *urn:be:fgov:ehealth:1.0:pharmacy:nihii-number*
- The identification of the pharmacy holder:
  - *urn:be:fgov:person:ssin:ehealth:1.0:pharmacy-holder*

Pharmacies must also specify which information must be asserted by the eHealth platform. To have access to the WS, the following data must be validated:

- The SSIN of the person starting the session : (AttributeNamespace: urn:be:fgov:identification-namespace)
  - *urn:be:fgov:ehealth:1.0:certificateholder:person:ssin*
  - *urn:be:fgov:person:ssin*
- The NIHII number of the pharmacy (the link between the pharmacy and the pharmacist starting the session is not verified, any pharmacist can start the session): (AttributeNamespace: urn:be:fgov:identification-namespace)
  - *urn:be:fgov:ehealth:1.0:pharmacy:nihii-number*
- The pharmacy must be a recognized pharmacy: (AttributeNamespace: urn:be:fgov:certified-namespace:ehealth)

[7] *OT : Office de tarification / TD : Tariferingsdienst*

- *urn:be:fgov:ehealth:1.0:pharmacy:nihii-number:recognisedpharmacy:boolean*

- The identification of the pharmacy holder (SSIN), i.e. the pharmacist responsible for all activities performed in the pharmacy: (AttributeNamespace: urn:be:fgov:identification-namespace)

  - *urn:be:fgov:person:ssin:ehealth:1.0:pharmacy-holder*

- The pharmacy holder must be the certified pharmacy holder of the given pharmacy: (AttributeNamespace: urn:be:fgov:certified-namespace:ehealth)

  - *urn:be:fgov:ehealth:1.0:pharmacy:nihii-number:person:ssin:ehealth:1.0:pharmacy-holder:boolean*

- To have access to the therapeutic link WS, the person must be a pharmacist: (AttributeNamespace: urn:be:fgov:certifiednamespace:ehealth)

  - *urn:be:fgov:person:ssin:ehealth:1.0:fpsph:pharmacist:boolean*

5.1.2.2 Healthcare professional

The request for the SAML token is secured with the eID[8] of the professional. The certificate used by the HOK verification mechanism is an eHealth certificate. The needed attributes are the following (AttributeNamespace: "urn:be:fgov:identification-namespace"):

- The social security identification number of the professional:

  - *urn:be:fgov:ehealth:1.0:certificateholder:person:ssin*
  - *urn:be:fgov:person:ssin*

For each professional, the following information must be asserted by eHealth :

- The social security identification number of the professional : (AttributeNamespace: "urn:be:fgov:identification-namespace")

  - *urn:be:fgov:ehealth:1.0:certificateholder:person:ssin*
  - *urn:be:fgov:person:ssin*

Depending on the professional category, other attributes may be asserted by the eHealth platform. These attributes are listed in the below sections.

5.1.2.2.1 Doctor

Doctor must also request this attribute:

- The NIHII number (11 positions) of the doctor (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"):

  - *urn:be:fgov:person:ssin:ehealth:1.0:doctor:nihii11*

5.1.2.2.2 Dentist

Dentist must also request this attribute:

- The NIHII number (11 positions) of the dentist (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"):

  - *urn:be:fgov:person:ssin:ehealth:1.0:dentist:nihii11*

5.1.2.2.3 Physiotherapist

Physiotherapist must also request this attribute:

- The NIHII number (11 positions) of the physiotherapist (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"):

[8] *As fall-back, in absence of the eID, the personal eHealth certificate can be used for authentication instead.*

- *urn:be:fgov:person:ssin:ehealth:1.0:physiotherapist:nihii11*

5.1.3 Security policies to apply

We expect that you use SSL one way for the transport layer.

As WS security policy, we expect:

- A timestamp (the date of the request), with a Time to live of one minute: if the message does not arrive during this minute, it shall not be treated).
- The signature with the certificate of
  - *the timestamp, (the one mentioned above)*
  - *the body (the message itself)*
  - *and the binary security token: an eHealth certificate or a SAML token issued by STS*

  This will allow the eHealth platform to verify the integrity of the message and the identity of the message author.

A document explaining how to implement this security policy can be obtained at the eHealth platform.

The STS cookbook can be found on the portal of the eHealth platform (Basic services).

5.2 Process overview

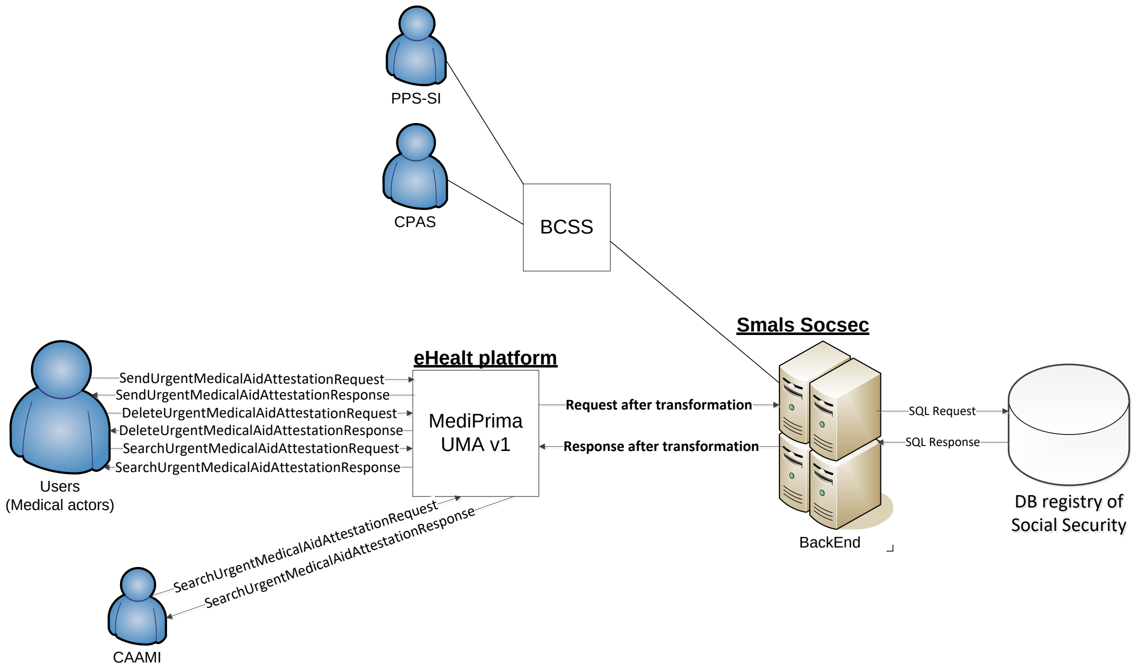

PPS-SI
CPAS
BCSS
Smals Socsec
eHealt platform
SendUrgentMedicalAidAttestationRequest
SendUrgentMedicalAidAttestationResponse
DeleteUrgentMedicalAidAttestationRequest
DeleteUrgentMedicalAidAttestationResponse
SearchUrgentMedicalAidAttestationRequest
SearchUrgentMedicalAidAttestationResponse
MediPrima UMA v1
Request after transformation
Response after transformation
SQL Request
SQL Response
Users (Medical actors)
BackEnd
DB registry of Social Security
SearchUrgentMedicalAidAttestationRequest
SearchUrgentMedicalAidAttestationResponse
CAAMI

Figure 2 : Process overview

5.3 Web service

- The language to construct the XML-messages is SOAP.
- The UMA attestation that a hospital/doctor sends to the registry concerns a single patient per message.

5.3.1 SendUrgentMedicalAidAttestation

This operation allows the user to send one attestation for a single patient in the UMA Attestations registry.

Note: The sender of the operation sendUrgentMedicalAidAttestation must be a hospital or a general doctor/dentist (in the future) in private practice.

5.3.1.1 Send Request

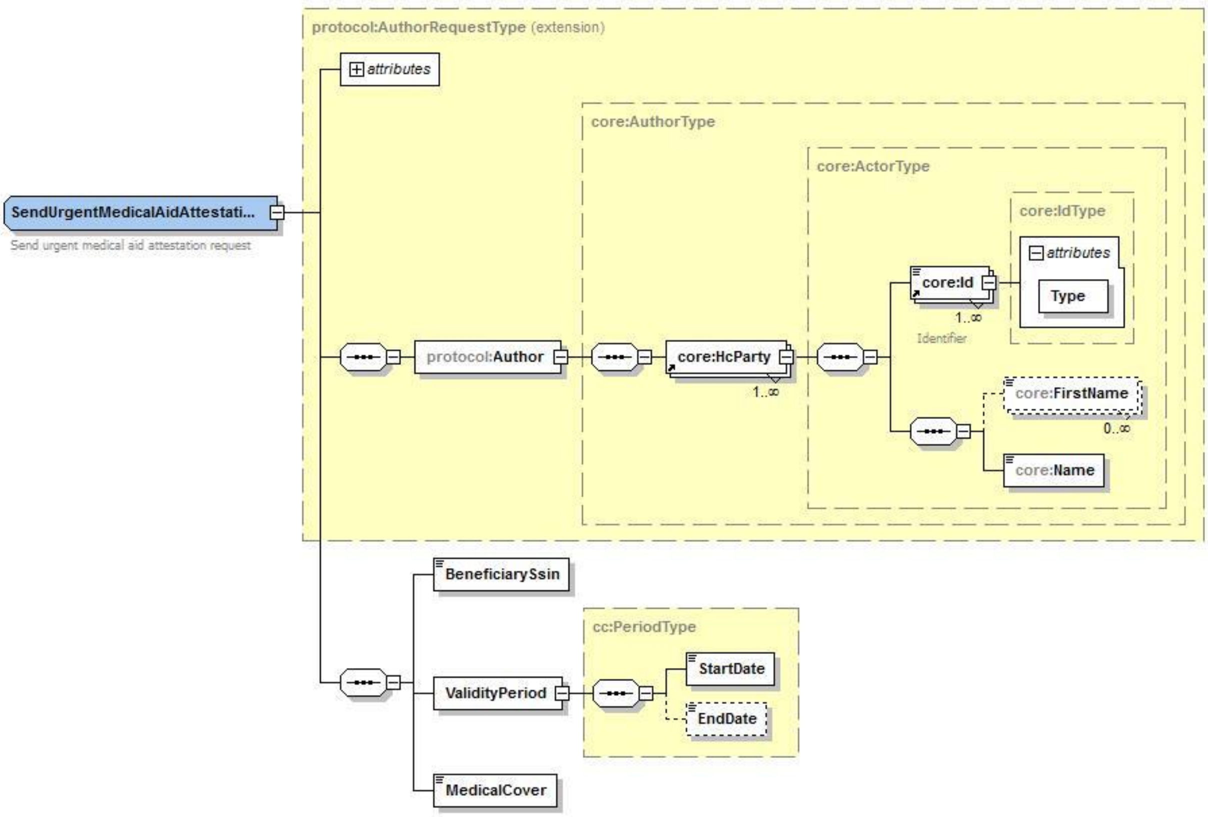


Figure 3 : SendUrgentMedicalAidAttestationRequest

Field name	Description
Author	• Author identifies the care provider who is responsible of the creation of the UMA (It is the prescriber, not the responsible of the sending). It is a medical actor with a NIHII number (11 positions) : doctor or dentist • *Cfr. AuthorType 5.3.4.1*
BeneficiarySsin	• BeneficiarySsin identifies the patient (foreigner) who is the beneficiary of the UMA attestation.
ValidityPeriod	• Period of validity of the attestation • The StartDate must be between current date and 45/60 days earlier • The EndDate must have a maximum value - Maximum one month in general cases - Maximum three months for hospitalization or paramedic *(cfr MedicalCover 5.3.4.2)* - If empty in input, the EndDate will be calculated automatically

<table>
<tr>
<td>MedicalCover</td>
<td>

- Type of the care concerning by the UMA attestation

<table>
<tr><th>Authorized value</th><th>Description</th></tr>
<tr><td>hospitalization</td><td>Hospitalization</td></tr>
<tr><td>ambulatoryhospitalization</td><td>Ambulatory hospitalization</td></tr>
<tr><td>doctor</td><td>Doctor</td></tr>
<tr><td>pharmaceuticaldrug</td><td>Pharmaceutical drug</td></tr>
<tr><td>paramedic</td><td>Paramedic</td></tr>
<tr><td>prosthesis</td><td>Prosthesis</td></tr>
<tr><td>medicaltransportation</td><td>Medical transportation</td></tr>
<tr><td>miscellaneous</td><td>Miscellaneous</td></tr>
</table>
</td>
</tr>
</table>

REMARK: Exactly one ‘Medical Cover’ for a patient per operation.

If multiple UMA attestations (with different medical cover) must be created for the same patient, then the operation ‘SendUrgentMedicalAidAttestation’must be repeated.

5.3.1.2 Send Response

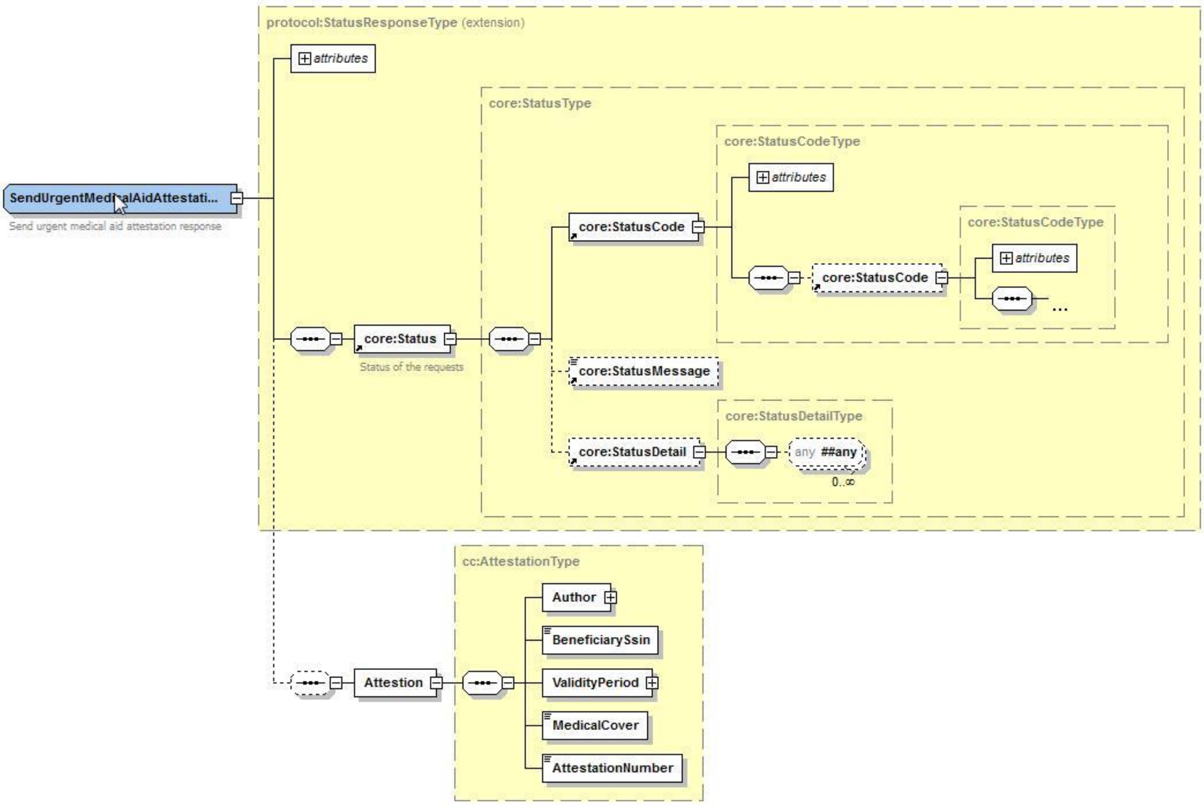


Figure 4 : SendUrgentMedicalAidAttestationResponse

Field name	**Description**
Status	• Status is the Status of the response • *Cfr StatusType 5.3.4.3*
Attestation	• The attestation resumes all information of the UMA attestation (Author, BeneficiarySsin, ValidityPeriod, MedicalCover) • Add an EndDate in ValidityPeriod if not indicated in the request • Add the AttestationNumber *(Cfr AttestationNumber 5.3.4.4)*

5.3.1.3 *Send Example*

The Header element in the example below is left empty in order to keep the example easy to read. A real request should always include the proper security *(Cfr 5.1.3 Security policies to apply)*.

A doctor with NIHII no 61013295790 and a name (Dupont) working in a hospital (UCL) with NIHII no 71089914 sends an UMA attestation. This attestation concerns a patient with NISS/Bis no 00122577811. This attestation is defined for a period of validity with a start date (2017-10-04), an end date (2017-10-04) and a medical cover (hospitalization).

Request:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSpy v2017 (x64) (http://www.altova.com)-->
<n2:SendUrgentMedicalAidAttestationRequest xmlns:core="urn:be:fgov:ehealth:commons:core:v2"
xmlns:protocol="urn:be:fgov:ehealth:commons:protocol:v2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:n2="urn:be:fgov:ehealth:mediprima:uma:protocol:v1" IssueInstant="2001-12-17T09:30:47Z"
xsi:schemaLocation="urn:be:fgov:ehealth:mediprima:uma:protocol:v1 ehealth-mediprima-uma-protocol-1_0.xsd">
        <protocol:Author>
                <core:HcParty>
                        <core:Id Type="urn:be:fgov:ehealth:1.0:physician:nihii-number">61013295790</core:Id>
                        <core:Name>Dupont</core:Name>
                </core:HcParty>
        </protocol:Author>
        <BeneficiarySsin>00122577811</BeneficiarySsin>
        </Beneficiary>
        <ValidityPeriod>
                <StartDate>2017-10-04</StartDate>
                <EndDate>2017-10-04</EndDate>
        </ValidityPeriod>
        <MedicalCover>hospitalization</MedicalCover>
</n2:SendUrgentMedicalAidAttestationRequest>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSpy v2017 (x64) (http://www.altova.com)-->
<core:SendUrgentMedicalAidAttestationResponse xmlns:core="urn:be:fgov:ehealth:commons:core:v2"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:core="urn:be:fgov:ehealth:mediprima:uma:protocol:v1" Id="ID1"
IssueInstant="2001-12-17T09:30:47Z" xsi:schemaLocation="urn:be:fgov:ehealth:mediprima:uma:protocol:v1 ehealth-mediprima-uma-
protocol-1_0.xsd">
        <core:Status>
                <core:StatusCode Value="urn:be:fgov:ehealth:2.0:Success"/>
        </core:Status>
        <core:Attestation>
                <core:Author>
                        <core:HcParty>
                                <core:Id Type="NIHIINbr">61013295790</core:Id>
                                <core:Name/>
                                </core:HcParty>
                </core:Author>
                <core:BeneficiarySsin>00122577811<core:BeneficiarySsin>
                </core:Beneficiary>
                <core:ValidityPeriod>
                        <core:StartDate>2017-10-04</core:StartDate>
                        <core:EndDate>2017-10-14</core:EndDate>
                </core:ValidityPeriod>
                <core:MedicalCover>hospitalization</core:MedicalCover>
                <core:AttestationNumber>690-HOSP-180000014652</core:AttestationNumber>
        </core:Attestation>
</core:SendUrgentMedicalAidAttestationResponse>
```

5.3.2 DeleteUrgentMedicalAidAttestation

This operation allows the user to delete an attestation in the UMA Attestations registry.

Before its deletion, an UMA attestation created has an **active** status. After a delete request *(and a success response for this request),* this attestation becomes **inactive.**

Note: The sender of the operation deleteUrgentMedicalAidAttestation must be a hospital or a general doctor / dentist (in the future) in private practice.

5.3.2.1 Delete Request

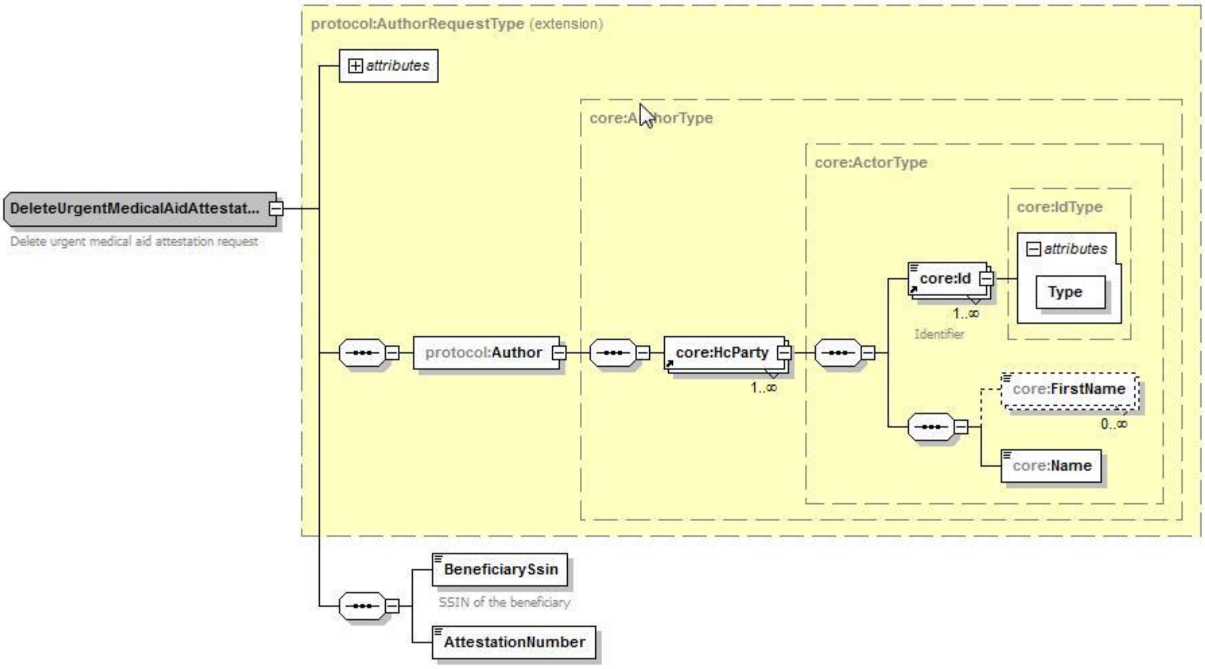


Figure 5 : DeleteUrgentMedicalAttestationRequest

Field name	Description
Author	• Author identifies the care provider who asks to delete the UMA. It's a medical actor with an INAMI number(11 positions): doctor or dentist. • *Cfr. AuthorType 5.3.4.1*
BeneficiarySsin	• SSIN is the NISS/Bis of the patient related to the UMA attestation to delete.
AttestationNumber	• AttestationNumber is the Attestation Number of the UMA attestation to delete

REMARK: The author of the deletion request must be the author of the original attestation.

5.3.2.2 Delete Response

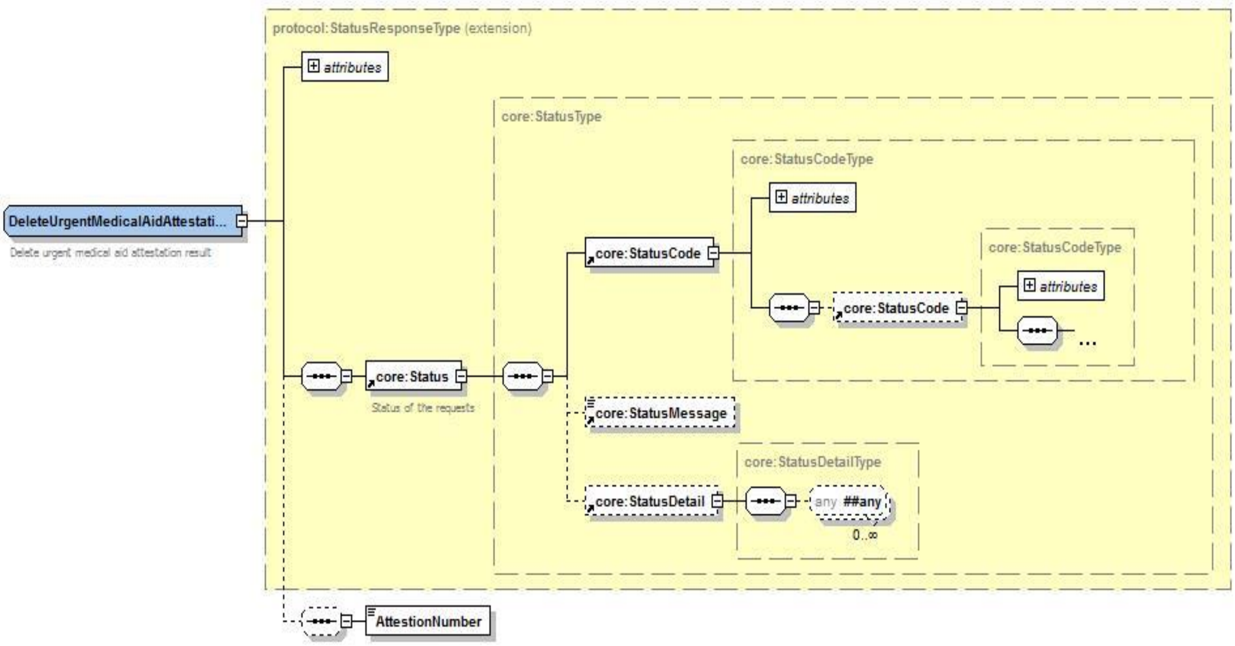


Figure 6 : DeleteUrgentMedicalAttestationResponse

Field name	Description
Status	• Status is the Status of the response • *Cfr StatusType 5.3.4.3*
AttestationNumber	• The AttestationNumber is the Attestation Number of the deleted UMA attestation.

5.3.2.3 Delete Example

The Header element in the example below is left empty in order to keep the example easy to read. A real request should always include the proper security *(Cfr 5.1.3 Security policies to apply)*.

A doctor with NIHII no 61013295790, and a name (Dupont) requests to delete UMA attestation no 690-HOSP-180000014652 related to the patient with NISS/Bis no 00122577811.

Request:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSpy v2017 (x64) (http://www.altova.com)-->
<n2:DeleteUrgentMedicalAidAttestationRequest xmlns:core="urn:be:fgov:ehealth:commons:core:v2"
xmlns:protocol="urn:be:fgov:ehealth:commons:protocol:v2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:n2="urn:be:fgov:ehealth:mediprima:uma:protocol:v1" IssueInstant="2001-12-17T09:30:47Z"
xsi:schemaLocation="urn:be:fgov:ehealth:mediprima:uma:protocol:v1 ehealth-mediprima-uma-protocol-1_0.xsd">
        <protocol:Author>
                <core:HcParty>
                        <core:Id Type="urn:be:fgov:ehealth:1.0:physician:nihii-number">61013295790</core:Id>
                        <core:Name>Dupont</core:Name>
                </core:HcParty>
        </protocol:Author>
        <BeneficiarySsin>00122577811</BeneficiarySsin>
        <AttestationNumber>690-HOSP-180000014652</AttestationNumber>
</n2:DeleteUrgentMedicalAidAttestationRequest>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSpy v2017 (x64) (http://www.altova.com)-->
<n2:DeleteUrgentMedicalAidAttestationResponse xmlns:core="urn:be:fgov:ehealth:commons:core:v2"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:n2="urn:be:fgov:ehealth:mediprima:uma:protocol:v1" Id="ID1"
IssueInstant="2001-12-17T09:30:47Z" xsi:schemaLocation="urn:be:fgov:ehealth:mediprima:uma:protocol:v1 ehealth-mediprima-uma-
protocol-1_0.xsd">
        <core:Status>
                <core:StatusCode Value=" urn:be:fgov:ehealth:2.0:Success"/>
        </core:Status>
        <core:AttestationNbr>690-HOSP-180000014652</core:AttestationNbr>
</n2:DeleteUrgentMedicalAidAttestationResponse>
```

5.3.3 SearchUrgentMedicalAidAttestation

This operation allows the user to search an attestation in the UMA Attestations registry.

Note: The sender of the operation searchUrgentMedicalAidAttestation must be a hospital or a general doctor / dentist (in the future) in private practice or a pharmacist.

5.3.3.1 Search Request

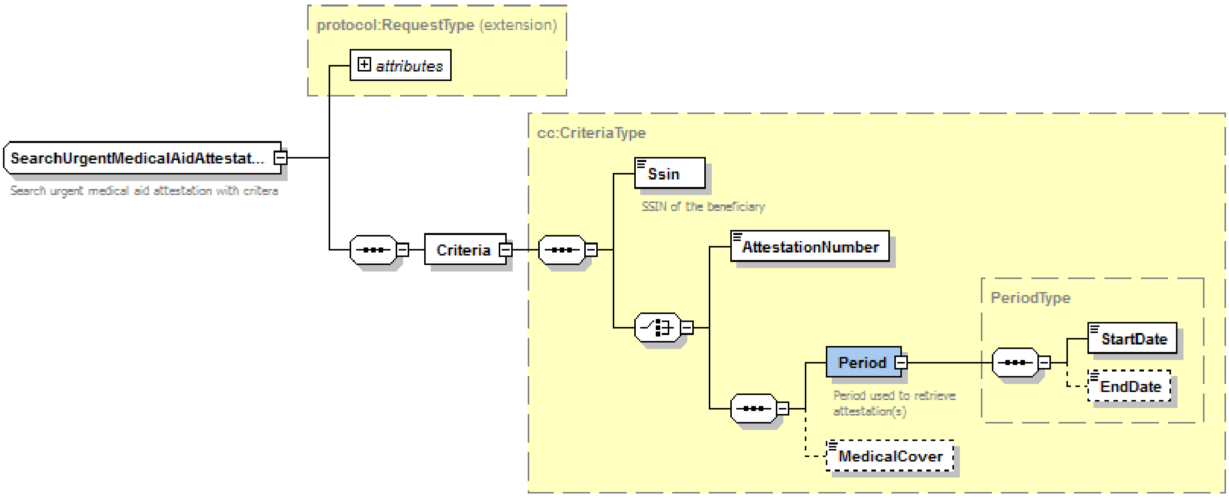

protocol:RequestType (extension)
attributes
SearchUrgentMedicalAidAttestat...
Search urgent medical aid attestation with critera
Criteria
cc:CriteriaType
Ssin
SSIN of the beneficiary
AttestationNumber
PeriodType
StartDate
EndDate
Period
Period used to retrieve attestation(s)
MedicalCover

Figure 7 : SearchUrgentMedicalAidAttestationRequest

Field name	Description
Criteria	• Criteria is a set of criteria used to search an UMA attestation. • *Cfr CriteriaType 5.3.4.5*

Note : A link between the sender of the search operation and the UMA attestation(s) must exists to retrieve the complete attestation → The sender must be the sender and/or the author of the original attestation.

For pharmacists: This restriction will not be applicable. They can only search for attestations with cover type 'pharmaceuticaldrug' (UMA attestation identifier = 690-**DRUG**-YYXXXXXXXXCC)

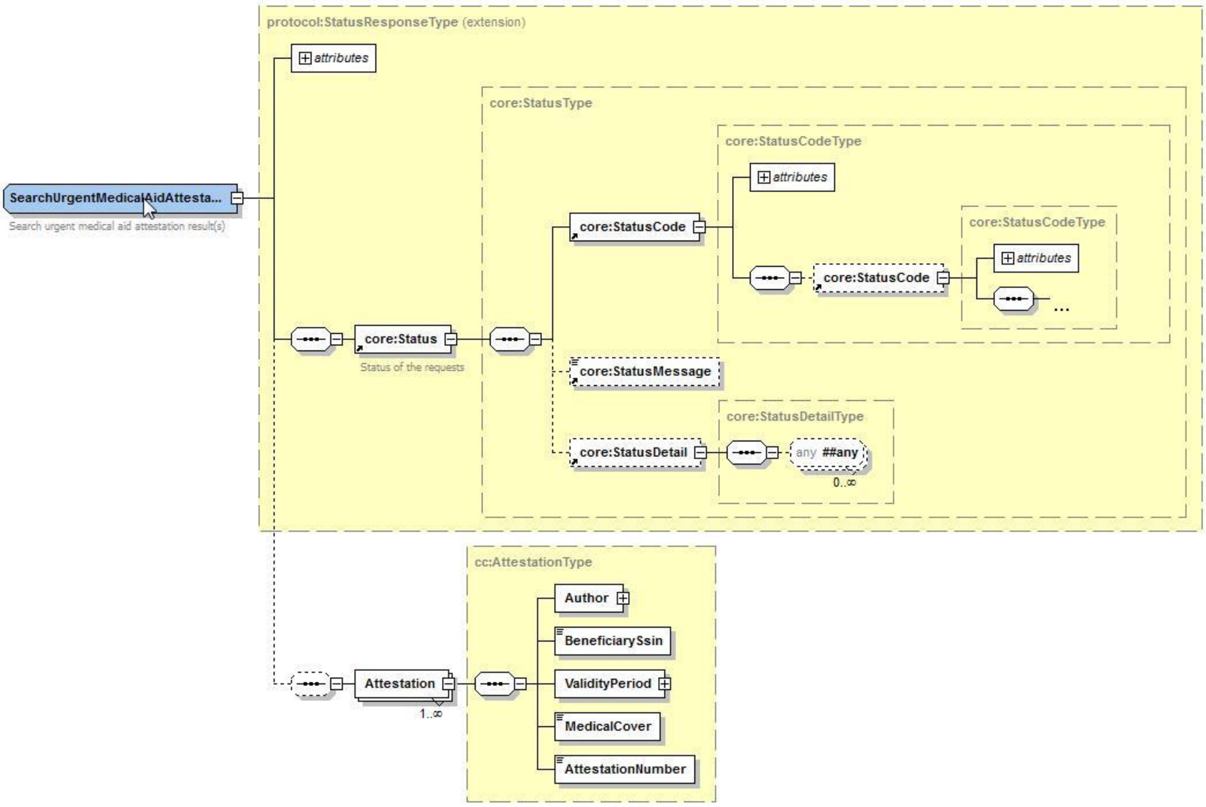


Figure 8 : SearchUrgentMedicalAidAttestationResponse

Field name	Description
Status	• Status is the Status of the response • *Cfr StatusType 5.3.4.3*
Attestation	• The Attestation resumes all information of the UMA attestation (Author, BeneficiarySsin, ValidityPeriod, MedicalCover, AttestationNumber) • A searching can find multiple attestations

5.3.3.2 *Search Example #1 (with AttestationNumber)*

The Header element in the example below is left empty in order to keep the example easy to read. A real request should always include the proper security *(Cfr 5.1.3 Security policies to apply)*.

A hospital with a NIHII number no 71089914 is searching for a specific UMA attestation. The attestation to retrieve is the attestation no 690-HOSP-180000014652 related to patient with NISS/Bis no 00122577811.

Request:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSpy v2017 (x64) (http://www.altova.com)-->
<n2:SearchUrgentMedicalAidAttestationRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:n2="urn:be:fgov:ehealth:mediprima:uma:protocol:v1" IssueInstant="2001-12-17T09:30:47Z"
xsi:schemaLocation="urn:be:fgov:ehealth:mediprima:uma:protocol:v1 ehealth-mediprima-uma-protocol-1_0.xsd">
        <Criteria>
                <Ssin>00122577811</Ssin>
                <AttestationNumber>690-HOSP-180000014652</AttestationNumber>
        </Criteria>
</n2:SearchUrgentMedicalAidAttestationRequest>
```

Reply:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSpy v2017 sp2 (x64) (http://www.altova.com)-->
<n2:SearchUrgentMedicalAidAttestationResponse xsi:schemaLocation="http://socialsecurity.be/urgentmedicalaidattestationregistry/v1
umaa_v1.xsd" xmlns:n2="http://socialsecurity.be/urgentmedicalaidattestationregistry/v1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:err="http://socialsecurity.be/errors/v1">
        <n2:Result>
                <n2:ResultCode>OK</n2:ResultCode>
        </n2:Result>
        <n2:Attestation>
                <n2:Author>

                        <n2:Id Type="NIHIINbr">61013295790</n2:Id><n2:Name/>
                        </n2:Author>
                <n2:BeneficiarySsin>00122577811</n2:BeneficiarySsin>
                <n2:ValidityPeriod>
                        <n2:StartingDate>2017-10-04</n2:StartingDate>
                        <n2:EndingDate>2017-10-13</n2:EndingDate>
                </n2:ValidityPeriod>
                <n2:MedicalCover>hospitalization</n2:MedicalCover>
                <n2:AttestationNbr>690-HOSP-180000014652</n2:AttestationNbr>
        </n2:Attestation>
</n2:SearchUrgentMedicalAidAttestationResponse>
```

5.3.3.3 *Search Example #2 (with Validity Period)*

The Header element in the example below is left empty in order to keep the example easy to read. A real request should always include the proper security *(Cfr 5.1.3 Security policies to apply)*.

A hospital with a NIHII no 71089914 is searching for UMA attestation(s) with medical cover ‘hospitalization’. The attestation(s) is (are) related to patient with NISS/Bis no 00122577811. At least one validity day of UMA attestation(s) must match to the period between StartDate (2017-10-05) and EndDate (2017-11-05)

Request:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSpy v2017 (x64) (http://www.altova.com)-->
<n2:SearchUrgentMedicalAidAttestationRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:n2="urn:be:fgov:ehealth:mediprima:uma:protocol:v1" IssueInstant="2001-12-17T09:30:47Z"
xsi:schemaLocation="urn:be:fgov:ehealth:mediprima:uma:protocol:v1 ehealth-mediprima-uma-protocol-1_0.xsd">
        <Criteria>
                <Ssin>00122577811</Ssin>
                <Period>
                        <StartDate>2017-10-05</StartDate>
                        <EndDate>2017-11-05</EndDate>
                </Period>
                <MedicalCover>hospitalization</MedicalCover>
        </Criteria>
</n2:SearchUrgentMedicalAidAttestationRequest>
```

Reply:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSpy v2017 (x64) (http://www.altova.com)-->
<core:SendUrgentMedicalAidAttestationResponse xmlns:core="urn:be:fgov:ehealth:commons:core:v2"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:core="urn:be:fgov:ehealth:mediprima:uma:protocol:v1" Id="ID1"
IssueInstant="2001-12-17T09:30:47Z" xsi:schemaLocation="urn:be:fgov:ehealth:mediprima:uma:protocol:v1 ehealth-mediprima-uma-
protocol-1_0.xsd">
        <core:Status>
                <core:StatusCode Value="urn:be:fgov:ehealth:2.0:Success"/>
        </core:Status>
        <core:Attestation>
                <core:Author>
                        <core:HcParty>
                                <core:Id Type="NIHIINbr">61013295790</core:Id>
                                <core:Name/>
                                </core:HcParty>
                </core:Author>
                <core:BeneficiarySsin>0012257781</core:BeneficiarySsin>
                <core:ValidityPeriod>
                        <core:StartDate>2017-10-04</core:StartDate>
                        <core:EndDate>2017-10-14</core:EndDate>
                </core:ValidityPeriod>
                <core:MedicalCover>hospitalization</core:MedicalCover>
                <core:AttestationNumber>690-HOSP-180000014652</core:AttestationNumber>
        </core:Attestation>
        <core:Attestation>
                <core:Author>
                        <core:HcParty>
                                <core:Id Type="NIHIINbr">61013295790</core:Id>
                                <core:Nam/e>
                        </core:HcParty>
                </core:Author>
                <core:BeneficiarySsin>0012257781</core:BeneficiarySsin>
                <core:ValidityPeriod>
                        <core:StartDate>2017-10-05</core:StartDate>
                        <core:EndDate>2017-11-05</core:EndDate>
                </core:ValidityPeriod>
                <core:MedicalCover>hospitalization</core:MedicalCover>
                <core:AttestationNumber>690-HOSP-180000014653</core:AttestationNumber>
        </core:Attestation>

</core:SendUrgentMedicalAidAttestationResponse>
```

5.3.4 Used Types

5.3.4.1 AuthorType

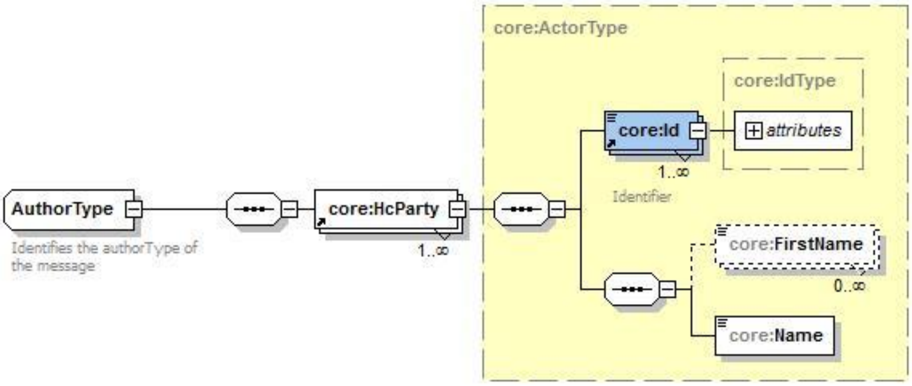


Figure 9 : AuthorType

Field name	Description
Id	• Id is the NIHII number to identify the Author. • Is[@Type] is the type of the NIHII.
FirstName	• FirstName of the Author.
Name	• Name of the Author.

<u>Possible category of authors:</u>

To send or delete an AMU attestation, the author must be a healthcare professional of a specific category. Current possibilities are 'doctor' and 'dentist'.

The category is defined by the inami (nihii) number type as specified in the following mapping tab:

	OutBound Category	Inbound Id[@Type]
Mapper	doctor	*urn:be:fgov:ehealth:1.0:physician:nihii-number*
	dentist	*urn:be:fgov:ehealth:1.0:dentist:nihii-number*

5.3.4.2 MedicalCover

MedicalCover is a string type that describes the type of an UMA attestation:

Authorized value	Description
hospitalization	Hospitalization
ambulatoryhospitalization	Ambulatory hospitalization
doctor	Doctor
pharmaceuticaldrug	Pharmaceutical drug
paramedic	Paramedic
prosthesis	Prosthesis
medicaltransportation	Medical transportation
miscellaneous	Miscellaneous

Exactly one type must be indicated.

5.3.4.3 *StatusType*

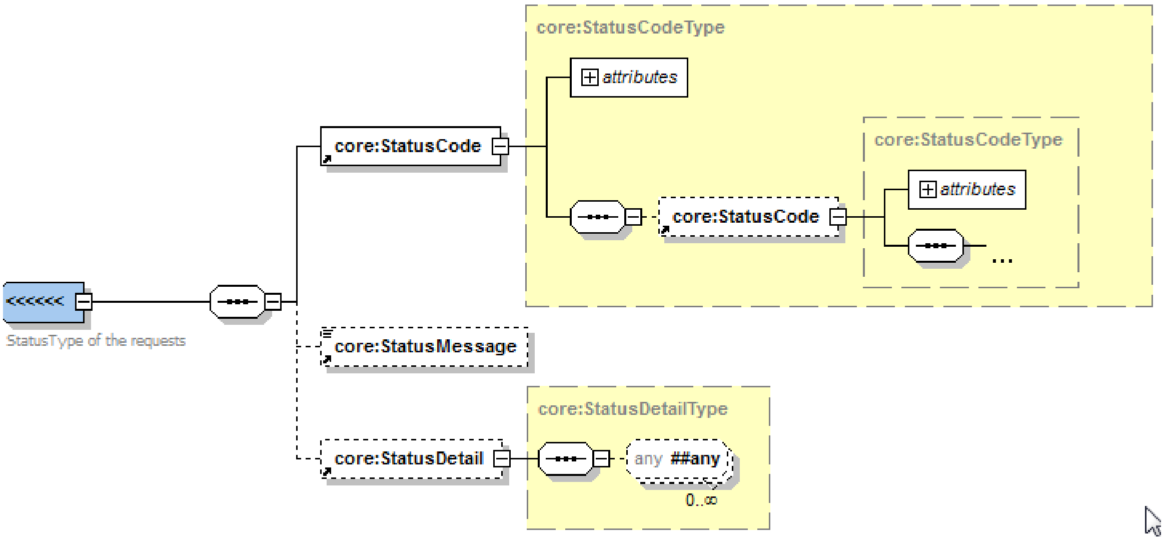


Figure 10 : StatusType

The SOA service response from the eHealth platform contains a Status element, used to indicate the status of the completion of the request. The status is represented by a StatusCode and optionally, the StatusMessage describing the status. An additional StatusDetail provides extra information on the encountered business errors returned by the target service.

- A StatusCode (level 1) *urn:be:fgov:ehealth:2.0:status:Success* indicates a success of the response.
- A StatusCode (level 1) *urn:be:fgov:ehealth:2.0:status:Requester* indicates the problem originates from the requestor. The requestor can therefore resolve it.
- A StatusCode (level 1) *urn:be:fgov:ehealth:2.0:status:Responder* indicates the problem originates from the eHealth platform WS. This might be due to a temporary unavailability.
- A statusCode (level 2) *urn:be:fgov:ehealth:2.0:status:MissingInput* indicates that some mandatory information is missing in the request.
- A statusCode (level 2) *urn:be:fgov:ehealth:2.0:status:RequestDenied* indicates something went wrong and the request was not processed. The StatusMessage might give more information on why the request was not processed.
- A statusCode (level 2) *urn:be:fgov:ehealth:2.0:status:Indeterminate* indicates an unknown error.
- A statusCode (level 2) *urn:be:fgov:ehealth:2.0:status:InvalidInput* indicates that some value in the request was not correct. The statusMessage might give more information.

Field name	Descriptions
StatusCode	• A StatusCode is recursive and can therefore contain an embedded StatusCode to define a sublevel statusCode. These codes can be used for automatic response handling. See table further for a list of possible values.
StatusMessage	• An optional message, describing the error. This message should never be used to automate the handling of a response and should therefore only be used as extra information next to the StatusCode.
StatusDetail	• The StatusDetail is defined as a free type, available for service to put any element in it to give extra information on the encountered business errors returned by the target service.

5.3.4.4 *AttestationNumber*

AttestationNumber is a string type that gives the unique number of an UMA attestation:

`VVV-TYPE-YYXXXXXXXXCC`

- VVV indicates the insurance organism
- TYPE* indicates the type of cover as mapped like this:

TYPE	Description
HOSP	Hospitalization
AMHO	Ambulatory hospitalization
DOCT	Doctor
DRUG	Pharmaceutical drug
PARA	Paramedic
PROS	Prosthesis
TRAN	Medical transportation
MISC	Miscellaneous

- YY = year of creation in the registry.
- XXXXXXXX corresponds to a sequence number.
- CC corresponds to a control number.

5.3.4.5 *CriteriaType*

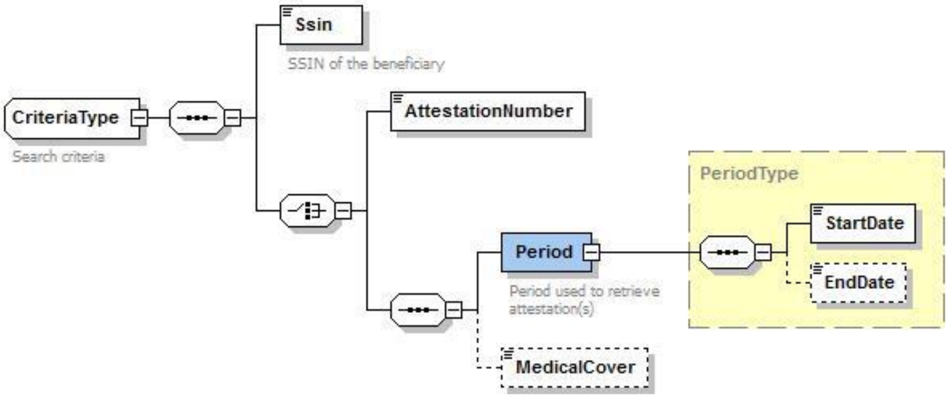


Figure 11 : CriteriaType

CriteriaType defines a set of criteria to search an UMA attestation. It contains the SSIN obligatory and some others information: the AttestationNumber OR Period + MedicalCover

Field name	Descriptions
Ssin	• SSIN is the NISS/Bis of the patient which we want to search his UMA attestation
AttestationNumber	• AttestationNumber is the number of the UMA that the user is searching. • *Cfr AttestationNumber 5.3.4.4*
Period	• Period defines a Period of time (StartDate and EndDate) of an UMA attestation that the user is searching.

MedicalCover	• MedicalCover is the type of an UMA attestation that the user is searching. • *Cfr 5.3.4.2*

6. Risks and security

6.1 Risks & safety

6.2 Security

6.2.1 Business security

In case the development adds an additional use case based on an existing integration, the eHealth platform must be informed at least one month in advance with a detailed estimate of the expected load. This will ensure an effective capacity management.

In case of technical issues on the WS, the partner may obtain support from the contact center (see Chap 3)

In case the eHealth platform finds a bug or vulnerability in its software, we advise the partner to update his application with the newest version of the software within 10 business days.

In case the partner finds a bug or vulnerability in the software or WS that the eHealth platform delivered, he is obliged to contact and inform us immediately. He is not allowed to publish this bug or vulnerability in any case.

6.2.2 Web service

WS security used in this manner is in accordance with the common standards. Your call will provide:

- SSL one way
- Time-to-live of the message: one minute.
- Signature of the timestamp, body and binary security token. This will allow the eHealth platform to verify the integrity of the message and the identity of the message author.
- No encryption on the message.

6.2.3 The use of username, password and token

The username, password and token are strictly personal. Partners and clients are not allowed to transfer them. Every user takes care of his username, password and token and he is forced to confidentiality of it. Moreover, every user is responsible of every use, which includes the use by a third party, until the inactivation.

7. Test and release procedure

7.1 Procedure

This chapter explains the procedures for testing and releasing an application in acceptation or production.

7.1.1 Initiation

If you intend to use the eHealth platform service, please contact ***info@ehealth.fgov.be***. The project department will provide you with the necessary information and mandatory documents.

7.1.2 Development and test procedure

You have to develop a client in order to connect to our WS. Most of the required integration info to integrate is published in the technical library on the portal of the eHealth platform.

Upon request, the eHealth platform provides you in some cases, with test cases in order for you to test your client before releasing it in the acceptance environment.

7.1.3 Release procedure

When development tests are successful, you can request to access the acceptance environment of the eHealth platform. From this moment, you start the integration and acceptance tests. The eHealth platform suggests testing during minimum one month.

After successful acceptance tests, the partner sends his test results and performance results with a sample of “eHealth request” and “eHealth answer” by email to his point of contact at the eHealth platform.

Then the eHealth platform and the partner agree on a release date. The eHealth platform prepares the connection to the production environment and provides the partner with the necessary information. During the release day, the partner provides the eHealth platform with feedback on the test and performance tests.

For further information and instructions, please contact: ***integration-support@ehealth.fgov.be***.

7.1.4 Operational follow-up

Once in production, the partner using the eHealth platform service for one of his applications will always test first in the acceptance environment before releasing any adaptations of its application in production. In addition, he will inform the eHealth platform on the progress and test period.

7.2 Test cases

The eHealth platform recommends performing tests for all of the following cases:

- SEND an UMA attestation.
- SEND an UMA attestation (with StartingDate + EndDate).
- SEND an UMA attestation (with a StartingDate but no EndDate).
- SEARCH an UMA attestation by its beneficiary ssin and attestation number.
- SEARCH an UMA attestation by its beneficiary ssin and StartingDate.
- SEARCH an UMA attestation by its beneficiary ssin, StartingDate, and EndDate.
- DELETE an UMA attestation.

In addition, the organization should also run negative test cases:

- Try to SEND an UMA attestation with a sender category not authorized to send.
- Try to SEND an UMA attestation with a sender not authorized to send.
- Try to SEND an UMA attestation with a dubble certificate authentification.
- Try to SEND an UMA attestation with an author’s nihii incorrect *(incorrect format – not 11 positions).*

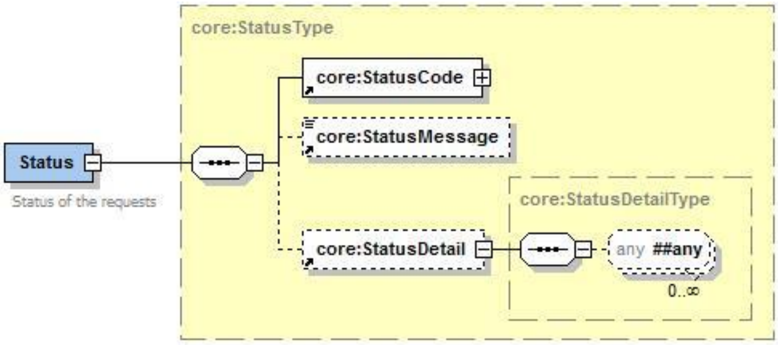
- Try to SEND an UMA attestation with an invalid author's category.
- Try to SEND an UMA attestation with an invalid beneficiary ssin *(incorrect format).*
- Try to SEND an UMA attestation with an invalid StartingDate *(StartingDate > current date).*
- Try to SEND an UMA attestation with an invalid EndDate (EndDate > StartingDate + 90 days for example).
- Try to SEND an UMA attestation with an invalid MedicalCover.
- Try to SEARCH an UMA attestation with a sender category not authorized to search.
- Try to SEARCH an UMA attestation with a sender not authorized to search.
- Try to SEARCH an UMA attestation with an invalid beneficiary ssin *(incorrect format).*
- Try to SEARCH an UMA attestation with a beneficiary ssin unknown in database.
- Try to SEARCH an UMA attestation with an incorrect attestation number.
- Try to SEARCH an UMA attestation with an attestation number unknown in database.
- Try to SEARCH an UMA attestation with an attestation number not linked to beneficiary.
- Try to SEARCH an inactive UMA attestation.
- Try to SEARCH an UMA attestation not linked to the sender.
- Try to SEARCH an UMA attestation with a bad StartingDate.
- Try to SEARCH an Uma attestation with a bad EndDate.
- Try to SEARCH an UMA attestation with a bad Medical cover.
- Try to DELETE an UMA attestation with a sender category not authorized to delete.
- Try to DELETE an UMA attestation with a sender not authorized to delete.
- Try to DELETE an UMA attestation with an author's nihii incorrect *(incorrect format).*
- Try to DELETE an UMA attestation with category of author <>doctor
- Try to DELETE an UMA attestation with an invalid beneficiary ssin *(incorrect format).*
- Try to DELETE an UMA attestation with a beneficiary ssin unknown in database.
- Try to DELETE an UMA attestation with an incorrect attestation number.
- Try to DELETE an UMA attestation with an attestation number unknown in database.
- Try to DELETE an UMA attestation with an attestation number not linked to beneficiary.
- Try to DELETE an UMA attestation not created by the author.
- Try to DELETE an inactive UMA attestation.

8. Error and failure messages

There are three different possible types of response:

- If there are no technical or business error, a business response is returned.
- If a business error occurred, it is contained in a business response.
- In the case of a technical error, a SOAP fault exception is returned.

8.1 Business errors



Possible business errors in the form of a Status response:

StatusCode	Message	Solution
urn:be:fgov:ehealth:2.0:status:Requester(level 1)	"Business particular error message"	Depends on the message. If the problem persists, contact SMALS support lines.
urn:be:fgov:ehealth:2.0:status:Requester(level 1)	MEDIPRIMA.UMA.ACCESS_NOT_PERMITTED : The sender of the request is an organization or a professional who's not authorized to use this application.	Use an organization or professional authorized to authenticate.
	MEDIPRIMA.UMA.DOUBLE_AUTH : You try to authentify you with more than one certificate.	Use an organization or professional (only one certificate) authorized to authenticate.
urn:be:fgov:ehealth:2.0:status:Responder(level 1)	Unexpected error of the service. Please contact service support	An unknown exception happened. Try again later, and if the problem persists, contact our support line.

Example:

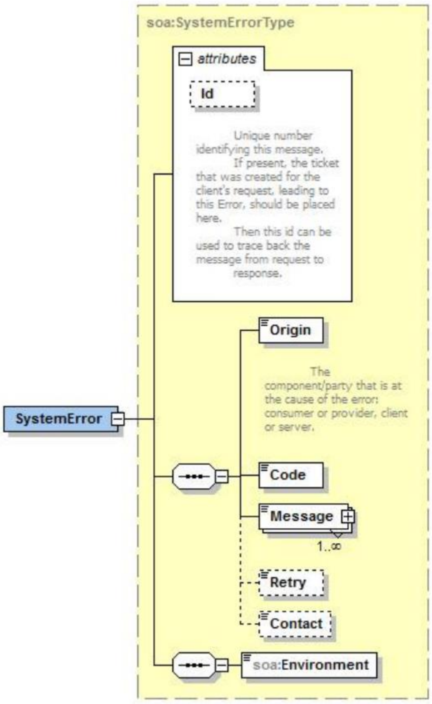
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Body xmlns:urn2="urn:be:fgov:ehealth:commons:core:v2" xmlns:urn1="urn:be:fgov:ehealth:commons:protocol:v2"
        xmlns:urn="urn:be:fgov:ehealth:mediprima:uma:protocol:v1" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
        utility-1.0.xsd" wsu:Id="id-405">
                <urn:SendUrgentMedicalAidAttestationResponse Id="_4121435b-2c05-4c89-bc81-4687e3849c90" InResponseTo="_f015df58-b07e-4643-
                a99b-3b3e" IssueInstant="2018-02-12T15:24:15.848+01:00">
                        <urn2:Status>
                                <urn2:StatusCode Value="urn:be:fgov:ehealth:2.0:Requester"/>
                                <urn2:StatusMessage>MEDIPRIMA.UMA.ACCESS_NOT_PERMITTED : The sender of the request is an organization
                                or a professional who's not authorized to use this application.</urn2:StatusMessage>
                        </urn2:Status>
                </urn:SendUrgentMedicalAidAttestationResponse>
        </soapenv:Body>
</soapenv:Envelope>
```

8.2 Technical errors

Error codes originating from the eHealth platform:

These error codes first indicate a problem in the arguments sent, or a technical error.

Technical errors are errors inherent to the internal working of a WS. They are returned as SOAP Faults. The SOA Standard for Errorhandling specifies a structure for SystemError and BusinessError, thrown as SOAP Faults. A SystemError MUST be thrown when a system failure occurred. It is not related to the business of the service. The SOA system error structure is as follows:


soa:SystemErrorType
attributes
Id
Unique number identifying this message. If present, the ticket that was created for the client's request, leading to this Error, should be placed here. Then this id can be used to trace back the message from request to response.
SystemError
Origin
The component/party that is at the cause of the error: consumer or provider, client or server.
Code
Message
1..∞
Retry
Contact
soa:Environment

The SystemError element contains a unique Id attribute for tracing. The Origin is set to Server or Provider. Retry is set to true if the user can try again immediately without interventions.

The SOAP Fault element has the following sub elements:

Element name	Description	Required
faultcode	A code for identifying the fault	Yes
faultstring	A human readable explanation of the fault	Yes
Faultactor	Information about who caused the fault to happen (the origin)	No
detail	Holds application specific error information related to the Body element. For example, it could include a java stack trace or any other kind of trace, used internally, to document on the cause of this error.	No

The default SOAP faultcode values are defined in an extensible manner that allows for new SOAP fault code values to be defined while maintaining backwards compatibility with existing fault code values.

Element name	Description
versionMismatch	Found an invalid namespace for the SOAP Envelope element.
mustUnderstand	An immediate Child element of the Header element, with the mustUnderstand attribute set to "1", was not understood.
Client	The message was incorrectly formed or contained incorrect information.
Server	There was a problem with the server so the message could not proceed.

Description of the possible SOAP fault exceptions:

Error code	Component	Description	Solution
SOA-00001	Undefined	Service error	This is the default error sent to the user in case further details are unknown.
SOA-01001	Consumer	Service call not authenticated	From the security information provided • or the user could not be identified • or the credentials provided are not correct
SOA-01002	Consumer	Service call not authorized	The user is identified and authenticated but is not allowed to call the given service.
SOA-02001	Provider	Service not available. Please contact service desk	An unexpected error has occurred • Retries will not work • Service desk may help with root cause analysis
SOA-02002	Provider	Service temporarily not available. Please try later	An unexpected error has occurred • Retries should work • If the problem persists service desk may help
SOA-03001	Consumer	Malformed message	This is default error for content related errors in case more details are missing.

SOA-03002	Consumer	Message must be SOAP	Message does not respect the SOAP standard
SOA-03003	Consumer	Message must contain SOAP body	Message respects the SOAP standard, but body is missing
SOA-03004	Consumer	WS-I compliance failure	Message does not respect the WS-I standard
SOA-03005	Consumer	WSDL compliance failure	Message is not compliant with WSDL in Registry/Repository
SOA-03006	Consumer	XSD compliance failure	Message is not compliant with XSD in Registry/Repository
SOA-03007	Consumer	Message content validation failure	From the message content (conform XSD): ● Extended checks on the element format failed ● Cross-checks between fields failed

Example:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Body>
                <soapenv:Fault>
                        <faultcode>soapenv:Server</faultcode>
                        <faultstring>SOA-00001: An internal error has occured. Please contact service desk.</faultstring>
                        <detail>
                                <urn:SystemError xmlns:urn="urn:be:fgov:ehealth:errors:soa:v1" Id="3d4fbb4b-3b53-49fa-8860-80cfe810bc38">
                                        <Origin>Server</Origin>
                                        <Code>SOA-00001</Code>
                                        <Message xml:lang="en">An internal error has occured. Please contact service desk.</Message>
                                        <urn:Environment>Test</urn:Environment>
                                </urn:SystemError>
                        </detail>
                </soapenv:Fault>
        </soapenv:Body>
</soapenv:Envelope>
```

Error message SOA-03004 will be thrown when the following rules are not satisfied.

Check	
R1008	An Envelope must not contain a Document Type Declaration.
R1032	The soap:Envelope, soap:Header, and soap:Body elements in an Envelope must not have attributes in the namespace **http://schemas.xmlsoap.org/soap/envelope/**
R2744	A HTTP request message must contain a SOAPAction a HTTP header field with a quoted value equal to the value of the soapAction attribute of soap:operation, if present in the corresponding WSDL description.
R2745	A HTTP request message must contain a SOAP action a HTTP header field with a quoted empty string value, if in the corresponding WSDL description, the SOAPAction of soapbind:operation is either not present, or present with an empty string as its value.