Attribute Authority WS
Cookbook
Version 1.7

This document is provided to you, free of charge, by the

eHealth platform

Willebroekkaai 38 – 1000 Brussel
38, Quai de Willebroeck – 1000 Bruxelles

Table of contents

1. Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1.00	06/07/2012	eHealth platform	First version
1.1	02/04/2014	eHealth platform	Added additional info in chapter SubjectConfirmationData
1.2	19/01/2017	eHealth platform	Updated chapter 5.1.1 (Security policies to apply) and 6.1.2 (Web Service)
1.3	21/03/2018	eHealth platform	Lay-out and links
1.4	04/02/2021	eHealth platform	WS-I Compliance Tracing
1.5	07/07/2021	eHealth platform	Update
1.6	13/07/2022	eHealth platform	§ 3.2 (Status (added) § 5.1.3 Tracing (updated)
1.7	25/01/2023	eHealth platform	Remove support for SHA-1

2. Introduction

2.1 Goal of the service

The “Attribute Authority (AA) web service (WS)” provided by the eHealth platform will allow our partners in the health sector to query the eHealth authentic source for health professional cadastre, file care providers, file care institutions, mandate, Responsibility Management for Public Health (ReMaPH), the National Registry of Belgian citizen data, …

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 eHealth service.

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

Technical and business requirements must be met in order to allow the integration and validation of the eHealth 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.[1]. 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

2.4 External document references

All documents can be found through the internet. They are available to the public, but not supported by the eHealth platform.

ID	Title	Source	Date	Author
1	saml-core-2.0-os	***http://docs.oasis-open.org/security/saml/v2.0/***	15/03/2005	Security Services TC
2	saml-profiles-2.0-os	***http://docs.oasis-open.org/security/saml/v2.0/***	15/03/2005	Security Services TC

[1] ***www.ehealth.fgov.be/ehealthplatform***

3	XML-Signature Syntax and Processing	***http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/Overview.html***	12/02/2002	IETF, W3C
4	Web Services Standardization Organization	***http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html***	24/0/2004	WS-I Org

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

The AA WS was built to separate access to the application from data access. This service's sole purpose is to return data.

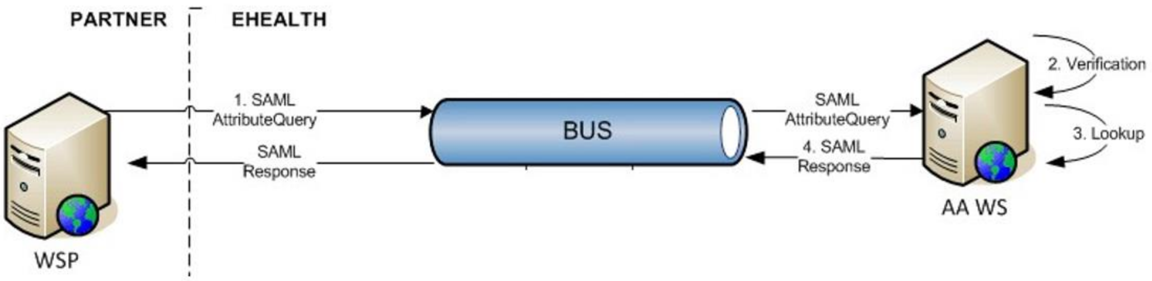


Figure 1

Step 1: A Web Service Consumer (WSC) sends a SAML AttributeQuery to the AA WS.

Step 2: The AA WS will verify if the WSC is registered as a valid user for the AttributeQuery that was sent and if the certificate in the header is valid.

Step 3: AA WS starts the lookup for the requested AttributeQuery and will return with a SAML Response.

Step 4: The AA WS sends a SAML Response to the WSC containing the requested data.

5. Step-by-step

5.1 Technical requirements

5.1.1 Security policies to apply

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

As web service security policy, we expect:

- A timestamp (the date of the request), with a Time to live of one minute.(if the message doesn't arrive during this minute, he 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 eHealth to verify the integrity of the message and the identity of the message author.

5.1.2 WS-I Basic Profile 1.1

Your request must be WS-I compliant (See Chap 2.4 – External document references).

5.1.3 Tracing

To use this service, the request SHOULD contain the following two http header values (see RFC ***https://datatracker.ietf.org/doc/html/rfc7231#section-5.5.3***):

1. User-Agent: information identifying the software product and underlying technical stack/platform. It MUST include the minimal identification information of the software such that the emergency contact (see below) can uniquely identify the component.
   a. Pattern: {minimal software information}/{version} {minimal connector information}/{connector-package-version}
   b. Regular expression for each subset (separated by a space) of the pattern: [[a-zA-Z0-9-\/]*\/[0-9azA-Z-_.]*
   c. Examples:
      User-Agent: myProduct/62.310.4 Technical/3.19.0
      User-Agent: Topaz-XXXX/123.23.X freeconnector/XXXXX.XXX
2. From**:** email-address that can be used for emergency contact in case of an operational problem
   Examples:
   From: *info@mycompany.be*

5.2 Description of xml-message

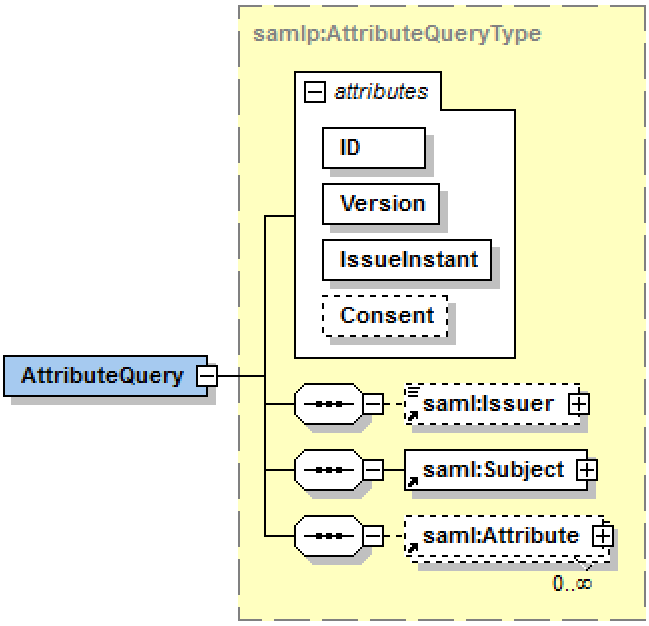
The different steps in Figure 1 are described here in more detail. The SAML AttributeQuery and SAML Response are open standards. This document will describe everything needed to contact the AA WS, but if you need more information than described in this document, we refer to reference 1 in § 2.4.

5.2.1 SAML AttributeQuery

The *<AttributeQuery>* element is used to make the query "Return the requested attributes for this subject". The "requested attributes" are those added to the *<Attribute>* element.

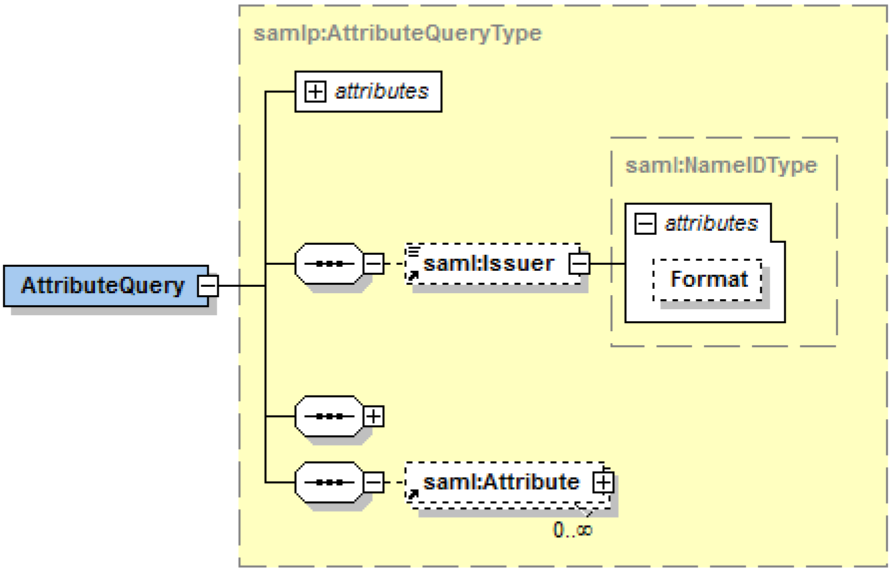
The *<AttributeQuery>* should be included inside the body of a signed SOAP Envelope.

5.2.1.1 AttributeQuery element



Attribute	Description
ID	The identifier for this attributeQuery (xs:ID).
Version	2.0
IssueInstant	The time instant of issue in UTC.
Consent	Indicates whether (and under what conditions) consent has been obtained from a principal in the sending of this request. See § 5.3.1.

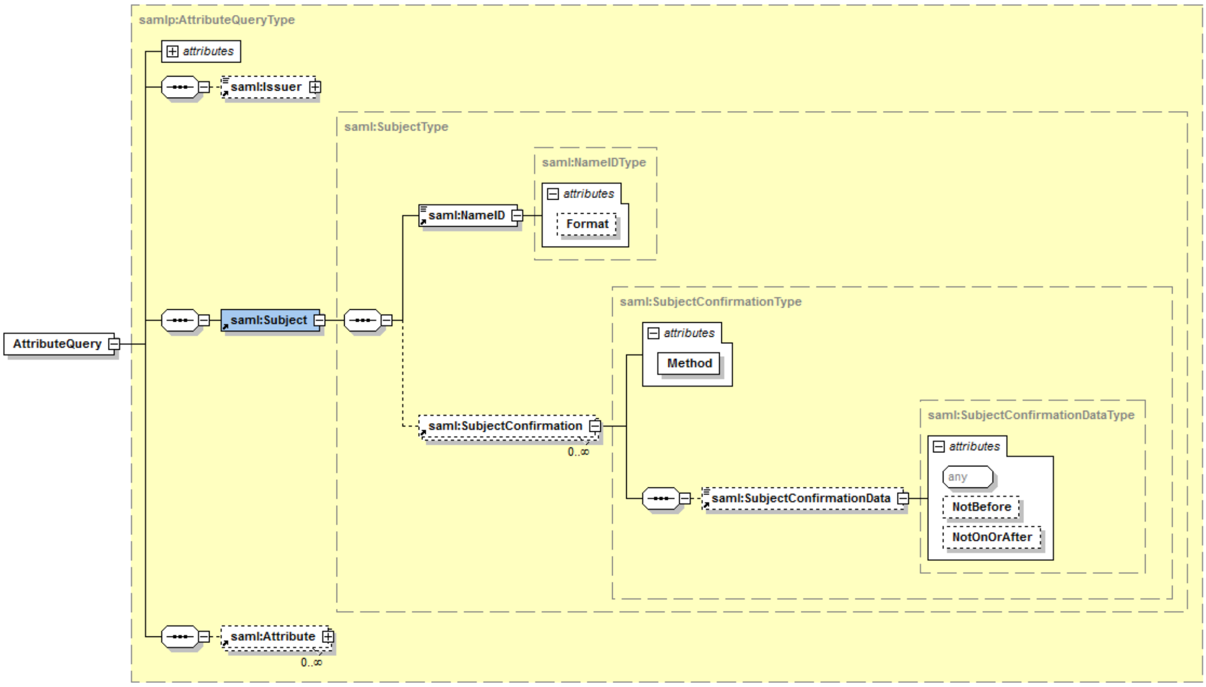
5.2.1.2 Issuer element



This element provides information about the issuer of the message. The element requires the use of an URI that can uniquely identify the requester.

Attribute	Description
Format	urn:oasis:names:tc:SAML:2.0:nameid-format:entity

5.2.1.3 *Subject element*



The *<Subject>* element defines the entity for which the issuer is requesting authentication or authorisation. The *<Subject>* element uses 2 sub elements (*<NameID>* and *<SubjectConfirmation>*), discussed below.

5.2.1.4 *NameID element*

The *<NameID>* value uniquely identifies the subject and has 2 attributes.

Attribute	Description
Format	A URI reference representing the classification of string-based identifier information. (See § 5.3.2)

5.2.1.5 *SubjectConfirmation element*

This is the information allowing the subject to be confirmed. The *Method* attribute is used to define how the confirmation was performed.

Attribute	Description
Method	The URI reference used to define how confirmation was performed. See § 5.3.3 for supported URIs.

5.2.1.6 *SubjectConfirmationData element*

The *<SubjectConfirmationData>* element specifies additional data (a specific timeframe) that allows the subject to be confirmed.

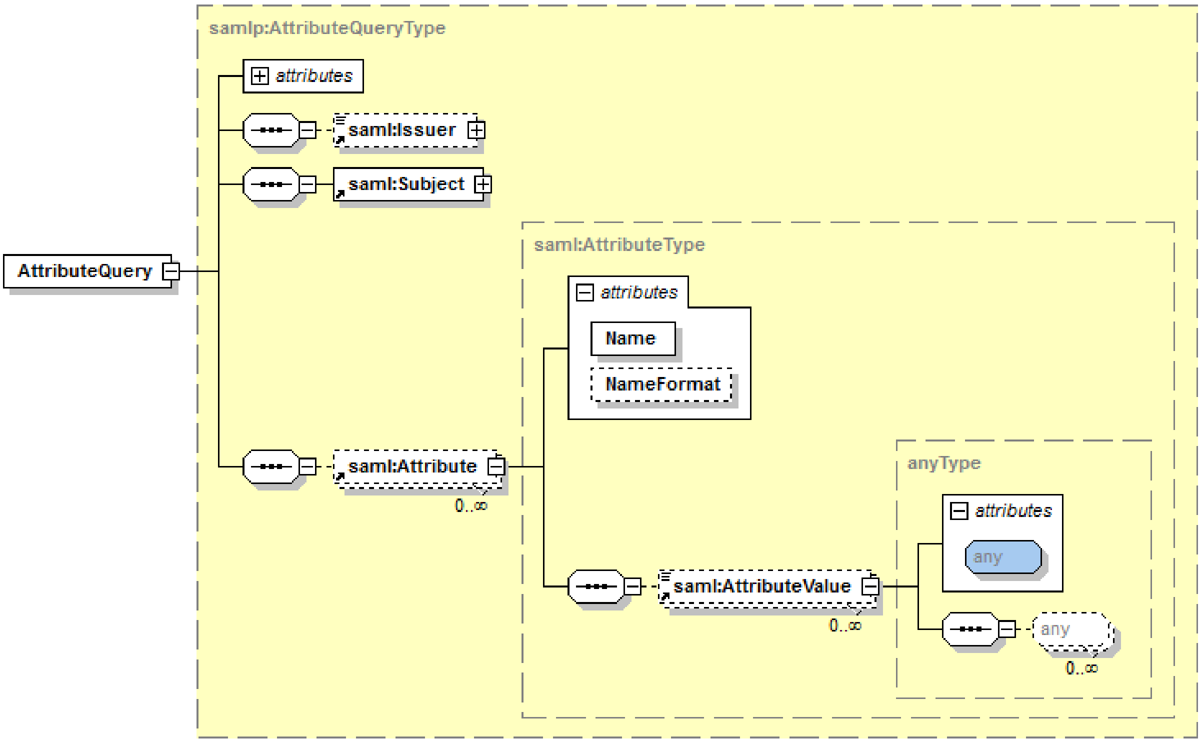
Attribute	Description
NotBefore	Optional - A time instance before which a subject cannot be confirmed. The time is encoded in UTC.
NotOnOrAfter	Optional - A time instance at which the subject can no longer be confirmed. The time value is encoded in UTC.

The following rules must be satisfied at any time:

- If the NotBefore or NotOnOrAfter attributes are present, their value must be a time encoded in UTC; otherwise the request will be rejected.
- The current date must be after NotBefore and before NotOnOrAfter, otherwise the request will be rejected. In other words, the current date must be between NotBefore and NotOnOrAfter. In some particular cases, the timeframe covered by NotBefore and NotOnOrAfter can be set in the past.
- If NotBefore is empty and NotOnOrAfter is not present, the request can be accepted.
- If NotBefore represents a date greater than the date contained in NotOnOrAfter, then the request will be rejected.
- If NotBefore is not empty and NotOnOrAfter is not present, the request can be accepted.

Point of attention: The specified timeframe is used to verify the assertions. Some attributes cannot be verified for a date bigger than today. This means you should be careful when sending an AttributeQuery around midnight.

5.2.1.7 Attribute element



<Attribute> elements are used to pass on additional information about the subject as well as specifying attributes whose value(s) is (are) to be returned.

An *<Attribute>* that does not contain an *<AttributeValue>* is information the requester does not have but needs. The AA WS will resolve these attributes and return them in the SAML Response.

An *<Attribute>* containing an *<AttributeValue>* is information that can be linked to the subject.

Attribute	Description
Name	Unique URI that identifies the attribute.
NameFormat	urn:oasis:names:tc:SAML:2.0:attrname-format:uri

5.2.1.8 *Example*

In the example below, we ask the AA WS if the person with SSIN 12345678901 and pharmacy NIHII number 12345678 is the pharmacy holder.

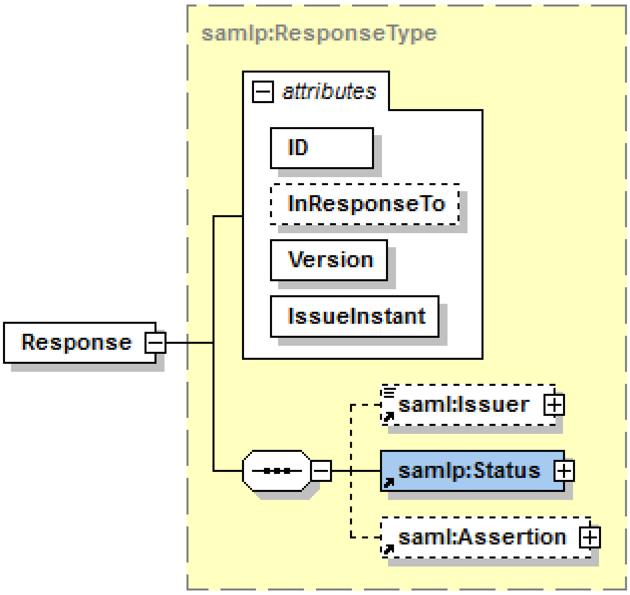
```
<samlp:AttributeQuery ID=" b59a2b546daff46daf89f5e9815f6e4b" Version="2.0" IssueInstant="
2012-07-04T09:47:01.182+02:00" Consent="urn:oasis:names:tc:SAML:2.0:consent:current-
implicit" xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:assertion ../saml20/xsd/saml-
schema-assertion-2.0.xsd urn:oasis:names:tc:SAML:2.0:protocol ../saml20/xsd/saml-schema-
protocol-2.0.xsd" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
         <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
urn:be:fgov:ehealth:supervision</saml:Issuer>
         <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient">252537746688268268547539284732423893</saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-
vouches">

<saml:SubjectConfirmationData NotBefore="2012-07-04T08:30:10+02:00"
 NotOnOrAfter="2012-07-04T09:30:10+02:00"/>
            </saml:SubjectConfirmation>
         </saml:Subject>
        <saml:Attribute Name="urn:be:fgov:person:ssin"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml:AttributeValue>12345678901</saml:AttributeValue>
         </saml:Attribute>
<saml:Attribute Name="urn:be:fgov:ehealth:1.0:pharmacy:nihii-number"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml:AttributeValue>12345678</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name=" urn:be:fgov:ehealth:1.0:pharmacy:nihii-
number:person:ssin:pharmacy-holder:nihii11"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                                    </samlp:AttributeQuery>
```

5.2.2 SAML Response

The SAML Response will be returned inside a SOAP Envelope. The response will include (but not limited to) a reference to the request, a status, a signature and attributes.

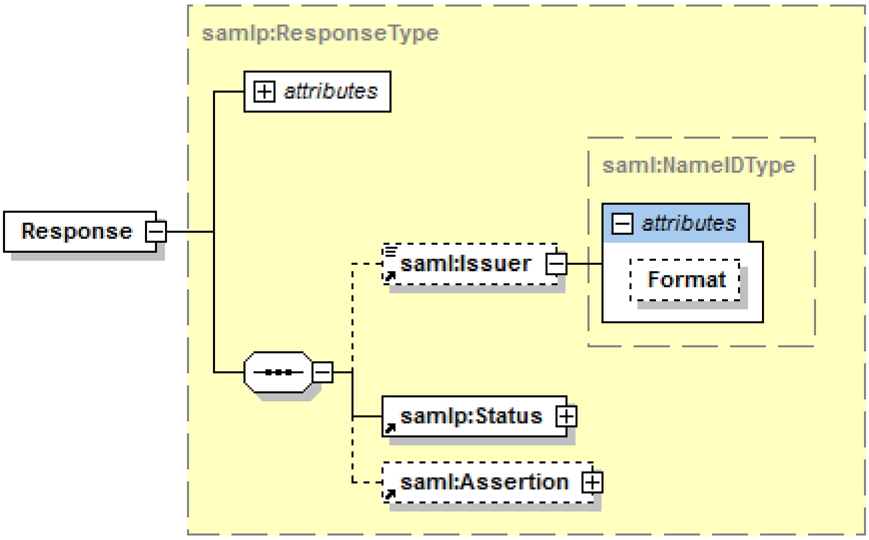
5.2.2.1 Response element



The attributes defined for the *<Response>* element can be used to trace back a response to the request it was built for.

Attribute	Description
ID	An identifier for the response.
InResponseTo	A reference to the identifier of the request to which the response corresponds.
Version	2.0
IssueInstant	The time instant of issue of the response in UTC.

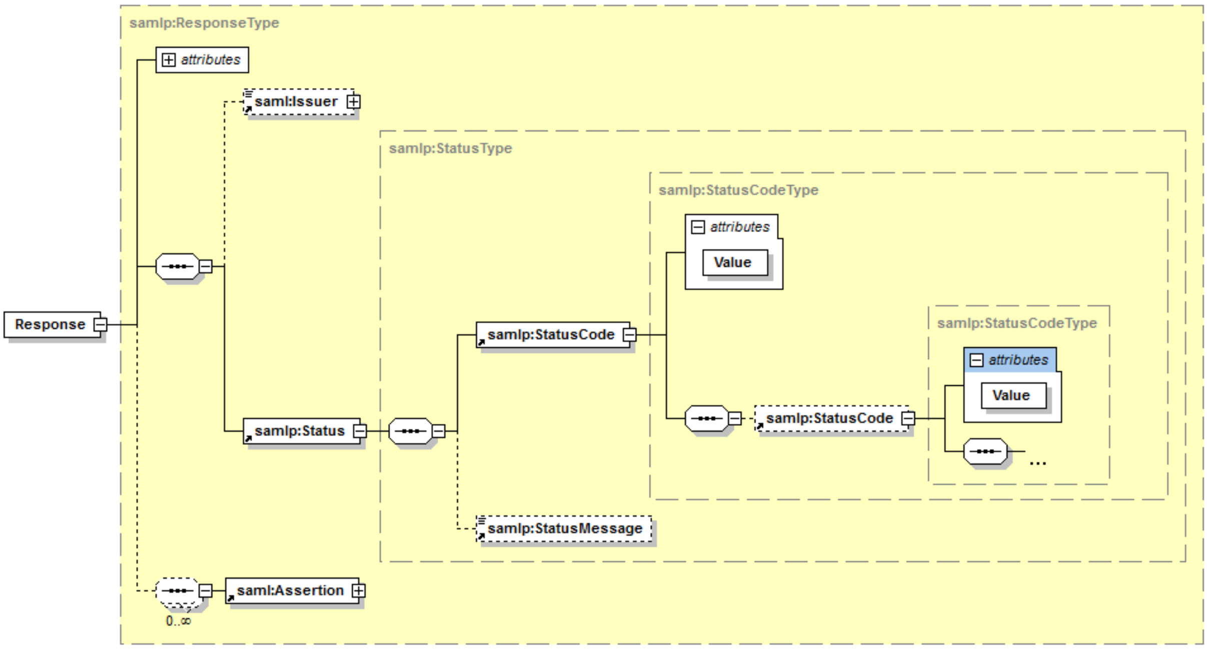
5.2.2.2 Issuer element



The *<Issuer>* element identifies the entity that generated the response message. This will always return *urn:be:fgov:ehealth:aa.*

Attribute	Description
Format	urn:oasis:names:tc:SAML:2.0:nameid-format:entity

5.2.2.3 Status element



The *<Status>* element represents the status of the corresponding request and contains a *<StatusCode>* element. In the case of an error, the *<StatusMessage>* element will also be present.

5.2.2.4 StatusCode element

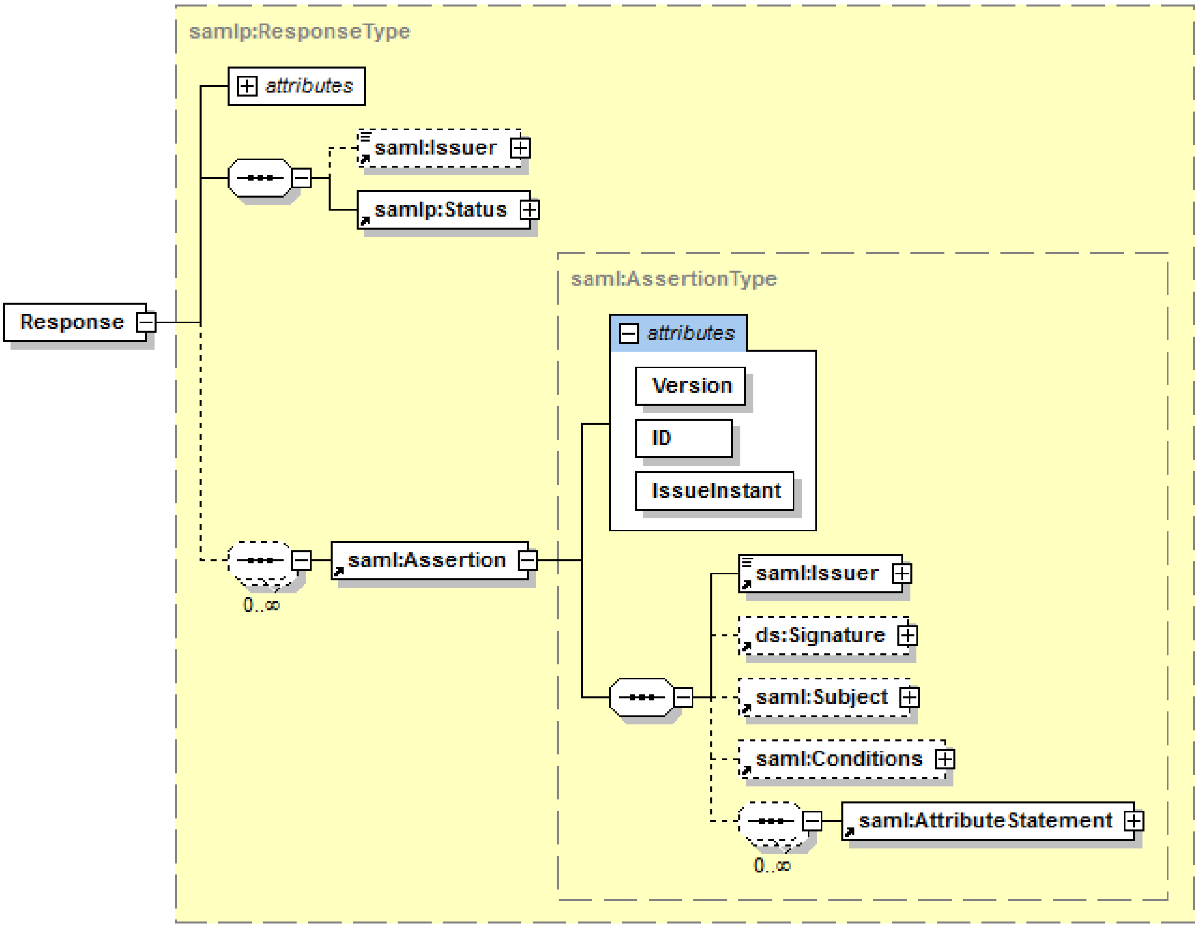
The code represents the status of the corresponding request. This can be a set of nested codes representing the status of the corresponding request.

Attribute	Description
Value	The status code value. The value of the topmost <*StatusCode>* element must be one from the top-level list provided in §5.3.4. The following second-level status codes can also be found in § 5.3.4.

5.2.2.5 StatusMessage element

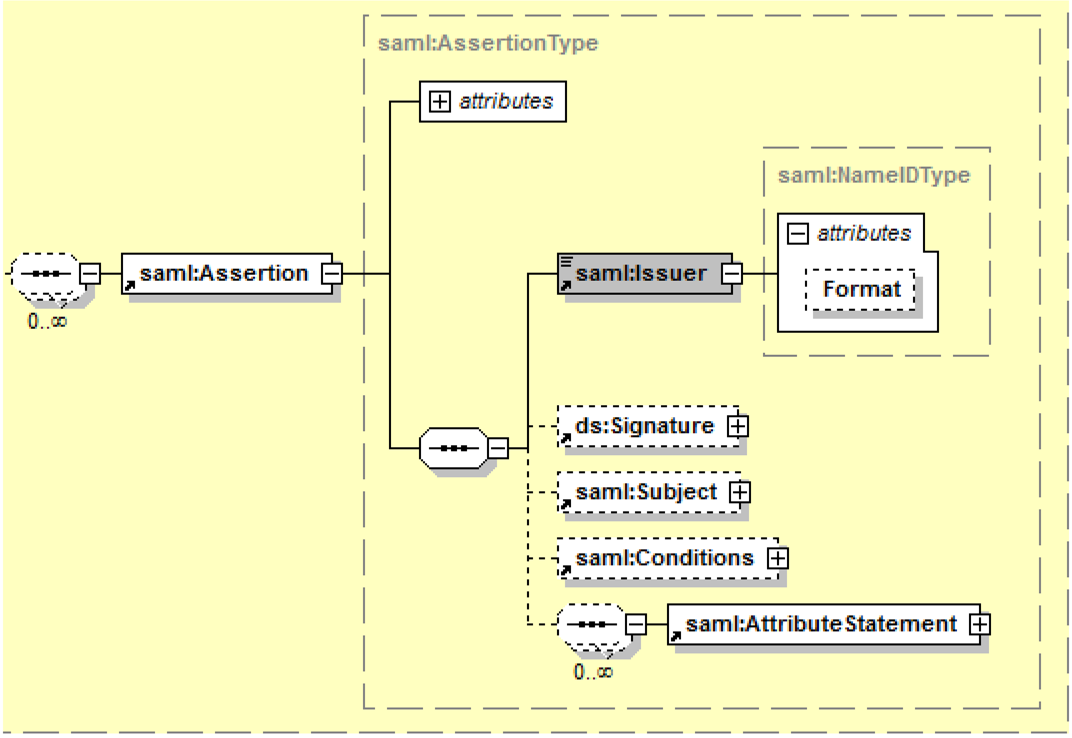
This message provides more info on the status.

5.2.2.6 *Assertion*



Attribute	Description
Version	2.0
ID	The identifier for this assertion
IssueInstant	The time instant of issue in UTC.

5.2.2.7 Issuer element



The SAML authority that is making the claim(s) in the assertion. This will always return *urn:be:fgov:ehealth:aa.*

Attribute	Description
Format	urn:oasis:names:tc:SAML:2.0:nameid-format:entity

5.2.2.8 Signature element

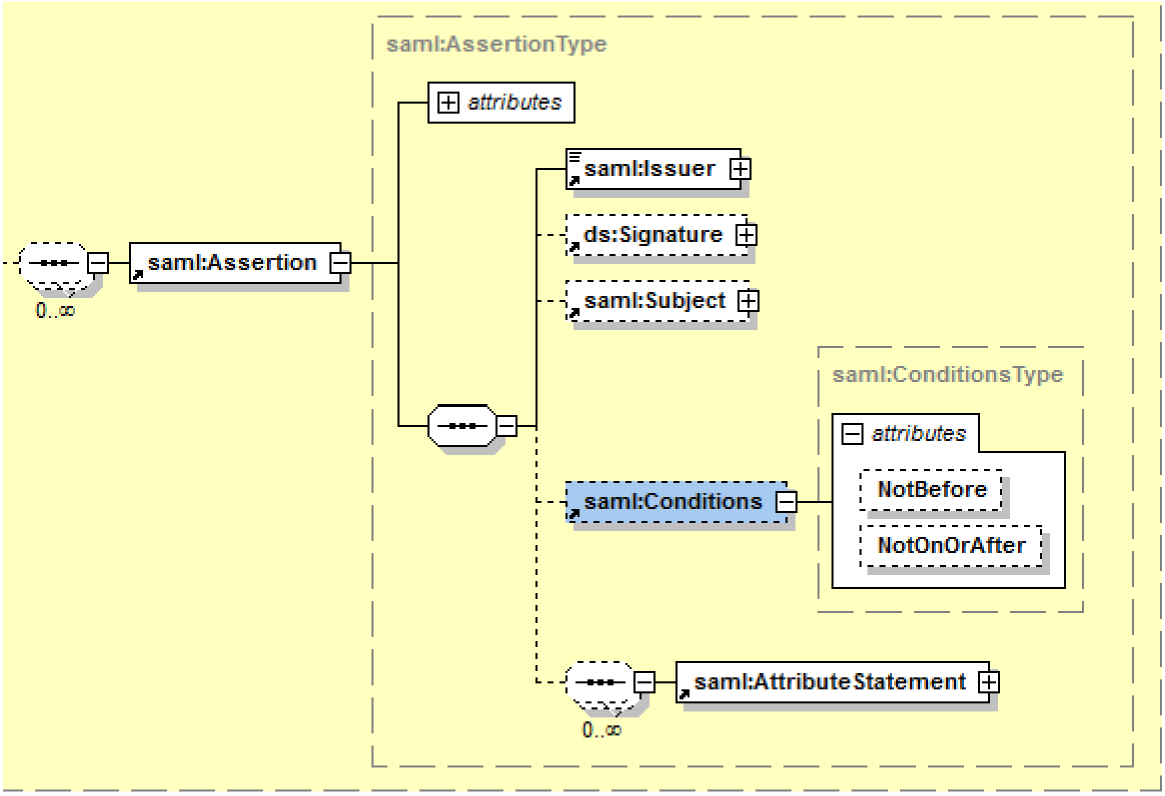
The *<Signature>* element is a default XML signature as specified by W3C (see reference 3 in 2.4), although only a subset is used for SAML Assertions. The signature should always be verified before processing the rest of the response. Detailed information about the *<Signature>* can be found in reference 3 of § 2.4 External document references.

The time being, only an x509v3 certificate is supported, information can be found in the KeyInfo/X509Data element.

5.2.2.9 Subject element

The *<Subject>* element references to the one sent in the request. See § 5.2.1.3.

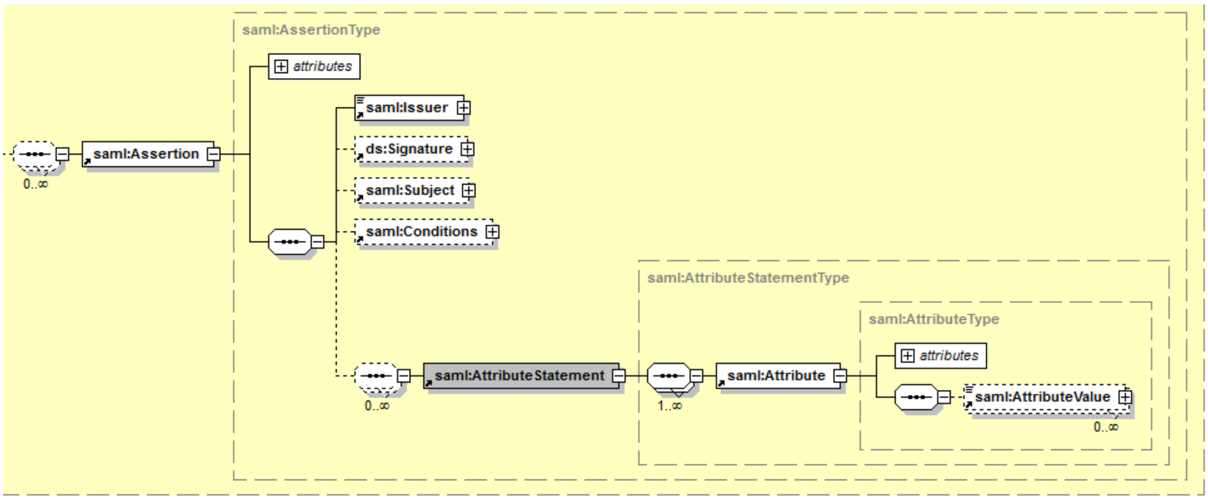
5.2.2.10 Conditions element



This element defines constraints on the acceptable use of SAML assertions.

Attribute	Description
NotBefore	Specifies the earliest time instant at which the assertion is valid. Encoded in UTC.
NotOnOrAfter	Specifies the time instant at which the assertion has expired. Encoded in UTC.

5.2.2.11 AttributeStatement element



The *<AttributeStatement>* element describes the statement by the AA WS asserting that the assertion subject is associated with the specified attributes. It contains *<Attribute>* elements.

5.2.2.12 Attribute element

The *<Attribute>* element is of the AttributeType complex type (see 0). These *<Attribute>* elements hold the response values to the *<Attribute>* elements contained in your request.

The value of the sub element *<AttributeValue>* can contain:

- xs:string: simple string
- xs:anyType: an inline well-formed XML
- empty: this means all processing to answer the request went fine, but no data was found

5.2.2.13 Example

In the example below, the issuer (AA WS) asserts that person with SSIN 12345678901 and pharmacy NIHII 12345678 is the pharmacy holder with NIHII number 12345678.

```
<ns3:Response ID="_3d6ad34bf46c0f84e72321917077a19c"
InResponseTo="b59a2b546daff46daf89f5e9815f6e4b" IssueInstant="2012-07-
04T07:56:21.159Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns3="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns5="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:ns6="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:ns7="urn:oasis:xacml:2.0:saml:assertion:schema:os"
  xmlns:ns8="urn:oasis:xacml:2.0:saml:protocol:schema:os">
  <Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">urn:be:fgov:ehealth:aa</Issuer>
  <ns3:Status>
     <ns3:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
                                    />
  </ns3:Status>
  <Assertion ID="_7e421a23b9dfee29cebb7e9cf0b25eef" IssueInstant="2012-07-
04T07:56:21.159Z" Version="2.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">urn:be:fgov:ehealth:aa</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc- c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>
        <ds:Reference URI="#_7e421a23b9dfee29cebb7e9cf0b25eef">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <ec:InclusiveNamespaces PrefixList="xs"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <ds:DigestValue>HwGjZmm05592QRqZaKBQaMl3Z3Q=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>adB….lm</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>I...Q</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
    <Subject>
      <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient">252537746688268268547539284732423893</NameID>
      <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-
      vouches">
        <SubjectConfirmationData NotBefore="2012-07-04T08:30:10+02:00"
NotOnOrAfter="2012-07-04T09:30:10+02:00" />
      </SubjectConfirmation>
    </Subject>
    <saml2:Conditions NotBefore="2012-07-04T07:56:21.167Z" NotOnOrAfter="2012-07-
04T08:01:21.167Z" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" />
    <AttributeStatement>
      <Attribute Name="urn:be:fgov:ehealth:1.0:pharmacy:nihii-number"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:urn1="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsu="http://docs.oasis- open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:xd="http://www.w3.org/2000/09/xmldsig#"
xmlns:xe="http://www.w3.org/2001/04/xmlenc#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">12345678
        </AttributeValue>
      </Attribute>
      <Attribute Name="urn:be:fgov:person:ssin"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:urn1="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsu="http://docs.oasis- open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:xd="http://www.w3.org/2000/09/xmldsig#"
xmlns:xe="http://www.w3.org/2001/04/xmlenc#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">12345678901
        </AttributeValue>
      </Attribute>
      <Attribute
Name="urn:be:fgov:ehealth:1.0:pharmacy:nihii-
number:person:ssin:pharmacy-holder:nihii11">
        <AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">23456789012</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertio
      n>

</ns3:Response>
```

5.3 Appendix

The appendix contains detailed information that can also be retrieved from the § 2.4 external document references. They are provided here for ease of use and are not exhaustive.

5.3.1 Consent

See also reference 1 in § 2.4 (saml-core-2.0-os.pdf) - section 8.4 for more info on the supported URIs.

urn:oasis:names:tc:SAML:2.0:consent:unspecified	No claim as to principal consent is being made.
urn:oasis:names:tc:SAML:2.0:consent:obtained	Indicates that the issuer of the message had obtained a principal's consent.
urn:oasis:names:tc:SAML:2.0:consent:prior	Indicates that the issuer of the message at some point prior to the action that initiated the message has obtained a principal's consent.
urn:oasis:names:tc:SAML:2.0:consent:current-implicit	Indicates that the issuer of the message has implicitly obtained a principal's consent during the action that initiated the message, as part of a broader indication of consent. Implicit consent is typically more proximal to the action in time and presentation than prior consent, such as part of a session of activities.
urn:oasis:names:tc:SAML:2.0:consent:current-explicit	Indicates that the issuer of the message had explicitly obtained a principal's consent during the action that initiated the message.
urn:oasis:names:tc:SAML:2.0:consent:unavailable	Indicates that the issuer of the message did not obtain consent.
urn:oasis:names:tc:SAML:2.0:consent:inapplicable	Indicates that the issuer of the message does not believe that they need to obtain or report consent.

5.3.2 NameID

See § 2.4 - reference 1 section 8.3 for more info on the URIs used.

urn:oasis:names:tc:SAML:2.0:nameid-format:transient	For requests where a memory id is used for the internal system itself; not to be used by the external system.
urn:oasis:names:tc:SAML:2.0:nameid-format:entity	For complex or system entities.
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	Unknown authentication method or id type.

5.3.3 Method

See § 2.4 - reference 2 - section 3 for more information.

urn:oasis:names:tc:SAML:2.0:cm:holder-of-key	The sender identifies himself in the subject and adds a key info element, linked to the private key he will use to sign the request. In this way, he proves he is the holder of the key.
urn:oasis:names:tc:SAML:1.0:cm:holder-of-key	
urn:oasis:names:tc:SAML:2.0:cm:sender-vouches	The sender vouches for the correctness of the subject and the responder can only trust the sender with a correctly identified subject.
urn:oasis:names:tc:SAML:1.0:cm:sender-vouches	

5.3.4 StatusCode

More info can be found in §2.4 – reference 1 (saml-core-2.0-os) § 3.2.2.2.

Top-level *<StatusCode>* values:

urn:oasis:names:tc:SAML:2.0:status:Success	The request succeeded.
urn:oasis:names:tc:SAML:2.0:status:Requester	Request not performed due to an error on the part of the requester.
urn:oasis:names:tc:SAML:2.0:status:Responder	Request not performed due to an error on the part of the SAML responder or SAML authority.
urn:oasis:names:tc:SAML:2.0:status:VersionMismatch	The SAML responder could not process the request because the version of the request message was incorrect.

The following second-level *<StatusCode>* values:

urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	The responding provider was unable to authenticate the principal.
urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue	Unexpected or invalid content was encountered within a <saml:Attribute> or <saml:AttributeValue> element.
urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy	The responding provider cannot or will not support the requested name identifier policy.
urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext	The responder cannot meet the specified authentication context requirements.
urn:oasis:names:tc:SAML:2.0:status:NoAvailableIDP	Used by an intermediary to indicate that none of the supported identity provider <Loc> elements in an <IDPList> can be resolved or that none of the supported identity providers are available.
urn:oasis:names:tc:SAML:2.0:status:NoPassive	Indicates the responding provider cannot authenticate the principal passively as has been requested.
urn:oasis:names:tc:SAML:2.0:status:NoSupportedIDP	Used by an intermediary to indicate that none of the identity providers in an <IDPList> are supported by the intermediary.

urn:oasis:names:tc:SAML:2.0:status:PartialLogout	Used by a session authority to indicate to a session participant that it was not able to propagate logout to all other session participants.
urn:oasis:names:tc:SAML:2.0:status:ProxyCountExceeded	Indicates that a responding provider cannot authenticate the principal directly and is not permitted to proxy the request further.
urn:oasis:names:tc:SAML:2.0:status:RequestDenied	The SAML responder or SAML authority is able to process the request but preferred not to respond. This status code MAY be used when there is concern about the security context of the request message or the sequence of request messages received from a particular requester.
urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	The SAML responder or SAML authority does not support the request.
urn:oasis:names:tc:SAML:2.0:status:RequestVersionDeprecated	The SAML responder cannot process any requests with the protocol version specified in the request.
urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooHigh	The SAML responder cannot process the request because the protocol version specified in the request message is a major upgrade from the highest protocol version supported by the responder.
urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooLow	The SAML responder cannot process the request because the protocol version specified in the request message is too low.
urn:oasis:names:tc:SAML:2.0:status:ResourceNotRec ognized	The resource value provided in the request message is invalid or unrecognized.
urn:oasis:names:tc:SAML:2.0:status:TooManyResponses	The response message would contain more elements than the SAML responder is able to return.
urn:oasis:names:tc:SAML:2.0:status:UnknownAttrProfile	An entity that has no knowledge of a particular attribute profile has been presented with an attribute drawn from that profile.
urn:oasis:names:tc:SAML:2.0:status:UnknownPrincip al	The responding provider does not recognize the principal specified or implied by the request.
urn:oasis:names:tc:SAML:2.0:status:UnsupportedBinding	The SAML responder cannot properly fulfil the request using the protocol binding specified in the request.

6. Risks and security

6.1 Security

6.1.1 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 web service 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.

6.1.2 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.

6.1.3 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 on the portal of the eHealth platform.

Upon request and depending on the case, the eHealth platform provides you with a ***test case*** 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

In order to test the service, the eHealth development team has to create a test case. The rules to access the AA WS are the same in test as in production.

The eHealth platform has to configure all test cases.

Before doing any tests, request your test cases from eHealth (***info@ehealth.fgov.be***). The form can be found on the portal of the eHealth platform (***https://www.ehealth.fgov.be/ehealthplatform/file/request_testcase_template***)

8. Error and failure messages

8.1 SOAP fault/error

See documentation ***SOA – Error guide***

8.2 SOAP Response (no SOAP fault)

If you do not receive a SOAP fault as described in Par 8.1, error codes returned by the eHealth platform for A.AM Attribute Authority can be found in the Status element of the response (See 5.3.4)