eHealth SSO
MyCareNet eAttest V2 WS

This document is provided to you free of charge by the

eHealth platform

Willebroekkaai 38 – Quai de Willebroeck 38

1000 BRUSSELS

Table of 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	25/02/2019	eHealth	Initial Version

2 Use of the eHealth SSO solution

The complete overview of the profile and a step-by-step implementation to start protecting a new application with SSO @ eHealth is described in the eHealth SSO cookbook.
This section specifies how the call to STS must be done to have access to the web service. You must precise several attributes in the request.

To access the eAttest web services, 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 eHealth to verify that the requested test cases were correctly configured.

The documents eAttest_STS_samlRequest.xml and eAttest_STS_samlResponse.xml provide STS request/response examples.

2.1 Healthcare professional

The request for the SAML token is secured with the eID[1] of the professional. The certificate used by the Holder-Of-Key (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* and *urn:be:fgov:person:ssin*

For each professional, eHealth has to assert the following information:

- The social security identification number of the professional : (AttributeNamespace: "urn:be:fgov:identification-namespace") urn:be:fgov:ehealth:1.0:certificateholder:person:ssin and urn:be:fgov:person:ssin

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

2.1.1 Doctor

Doctor must also request this attribute in the AttributeQuery :

- The NIHII number of the doctor (AttributeNamespace: "*urn:be:fgov:certified-namespace:ehealth*"): *urn:be:fgov:person:ssin:ehealth:1.0:doctor:nihii11*

2.1.2 Dentist

Dentist must also request this attribute in the AttributeQuery :

[1] As fallback, in absence of the eID, the personal eHealth certificate can be used for authentication instead.

- The NIHII number of the doctor (AttributeNamespace: "*urn:be:fgov:certified-namespace:ehealth*"): *urn:be:fgov:person:ssin:ehealth:1.0:dentist:nihii11*

2.2 Healthcare institution

The SAML token request is secured with the eHealth certificate of the institution. The certificate used by the HOK verification mechanism is the same eHealth certificate. The needed attributes depend on the institution type (for example: hospital, labo, group of nurses, …).

2.2.1 Guard post

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

- The NIHII number of the guard post:
  - *urn:be:fgov:ehealth:1.0:guardpost:nihii-number*
  - *urn:be:fgov:ehealth:1.0:certificateholder:guardpost:nihii-number*

The healthcare institution must also specify which information must be asserted by eHealth:

- The NIHII number of the healthcare institution (AttributeNamespace: “urn:be:fgov:identification-namespace”):
  - *urn:be:fgov:ehealth:1.0:guardpost:nihii-number*
  - *urn:be:fgov:ehealth:1.0:certificateholder:guardpost:nihii-number*
- The healthcare institution must be recognized (AttributeNamespace: urn:be:fgov:certifiednamespace:ehealth):

  urn:be:fgov:ehealth:1.0:certificateholder:guardpost:nihii-number:recognisedguardpost:boolean
- The NIHII number (11 positions) of the healthcare institution (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"):

  urn:be:fgov:ehealth:1.0:guardpost:nihii-number:recognisedguardpost:nihii11

2.3 Mandate holder

2.3.1 Mandated organization

The SAML token request is secured with the eHealth certificate of the mandated organization. The certificate used by the HOK verification mechanism is the same eHealth certificate. The needed attributes are the following (AttributeNamespace: "*urn:be:fgov:identification-namespace*"):

- The CBE number of the mandated organization:
  - *urn:be:fgov:ehealth:1.0:certificateholder:enterprise:cbe-number*
  - *urn:be:fgov:kbo-bce:organization:cbe-number*

Mandated organization must also specify which information must be asserted by eHealth:

- The CBE number of the mandated organization (AttributeNamespace: "urn:be:fgov:identification-namespace"):
  - *urn:be:fgov:ehealth:1.0:certificateholder:enterprise:cbe-number*
  - *urn:be:fgov:kbo-bce:organization:cbe-number*

- The mandated organization must be a recognized mandated organization (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"):

  urn:be:fgov:kbo-bce:organization:cbe-number:ehealth:1.0:recognisedmandatary:boolean

- The service name :

  urn:be:fgov:ehealth:1.0:servicename:external with the value 'attest'

2.3.2 Mandated person

The request for the SAML token is secured with the eID[2] of the mandated person. 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 mandated person:
  - *urn:be:fgov:ehealth:1.0:certificateholder:person:ssin*
  - *urn:be:fgov:person:ssin*

Mandated person must also specify which information must be asserted by eHealth:

- The social security identification number of the mandated person: (AttributeNamespace: "urn:be:fgov:identification-namespace") :
  - *urn:be:fgov:ehealth:1.0:certificateholder:person:ssin*
  - *urn:be:fgov:person:ssin*
- The person must be a recognized mandated person: (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth")

  urn:be:fgov:person:ssin:ehealth:1.0:recognisedmandatary:boolean

- The service name (AttributeNamespace: "urn:be:fgov:identification-namespace"):

  urn:be:fgov:ehealth:1.0:servicename:external
  with the value 'attest'

[2] As fallback, in absence of the eID, the personal eHealth certificate can be used for authentication instead.