eHealth SSO
MyCareNet Tarification

This document is provided to you free of charge by the

eHealth platform

Willebroekkaai 38 – Quai de Willebroeck 38
1000 BRUSSELS

All are free to circulate this document with reference to the URL source.

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	11/04/2014	eHealth	First version
2	07/09/2016	eHealth	Update with new target groups

2 Use of the eHealth SSO solution

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

To access the MyCareNet tarification web service (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 "false" for one boolean certification attributes
- do not obtain any value for one of the nihii11 certification attributes

then you should contact eHealth to verify whether the requested test cases were configured in the right way.

The documents "Tarification_STS_samlRequest.xml" and "Tarification_STS_samlResponse.xml" provide STS request/response examples.

Currently, only general practitioners (or their mandate-holder) can access the tarification service.

In order to facilitate the Single-Sign-On (SSO) the SAML tokens as described in this section (doctor as individual) are the same as for some other services which are used by the general practitioners (e.g. MyCareNet GMF Notification service, MyCareNet Registration service).

2.1 Healthcare professional

The request for the SAML token is secured with the professional's eID[1]. The certificate used by the Holder-Of-Key (HOK) verification mechanism is an eHealth certificate. The required 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*
- The user uses his/her personal certificate (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:ehealth:1.0:certificateholder:person:ssin:usersession:boolean

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

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

2.1.1 Doctor as individual

Doctor as individual 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 as individual

Dentist must also request this attribute in the AttributeQuery:

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

2.2 Doctor within a hospital

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

- The social security identification number of the doctor: urn:be:fgov:person:ssin
- The NIHII number of the hospital:
  - *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number*
  - *urn:be:fgov:ehealth:1.0:hospital:nihii-number*

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

- The social security identification number of the doctor (AttributeNamespace: "urn:be:fgov:identification-namespace"): urn:be:fgov:person:ssin
- The NIHII number of the hospital:
  - *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number*
  - *urn:be:fgov:ehealth:1.0:hospital:nihii-number*
- The NIHII number of the doctor (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:person:ssin:ehealth:1.0:doctor:nihii11
- The hospital must be a recognized hospital (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"):
  - *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number:recognisedhospital:boolean*

2.3 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 institution type defines the required attributes.

2.3.1 Guard post

The required 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*

2.4 Mandate holder

2.4.1 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 required 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 ‘insurability’*

2.4.2 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 required 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 persons have also to 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 user uses his/her personal certificate
  (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"):
  urn:be:fgov:ehealth:1.0:certificateholder:person:ssin:usersession:boolean
- 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 'insurability'*

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