Chapter IV
SSO
Version 1.5

This document is provided to you free of charge by the

eHealth platform
Willebroekkaai 38 – 1000 Brussel
38, Quai de Willebroek – 1000 Bruxelles

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
1.3	08/12/2011	eHealth platform	
1.4	31/05/2021	eHealth platform	Update
1.5	09/07/2025	eHealth platform	Remove SAML sender-vouches solution Remove deprecated information (AttributeNamespace)

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 Secure Token Service (STS) must be done to have access to the web service. You must precise several attributes in the request.

To access the Chapter IV 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 "false" for one boolean certification attributes;
- you do not obtain any value for one of the nihii11 certification attributes;

then contact eHealth to verify that the requested test cases were correctly configured.

2.1 Health care professional

2.1.1 Physician

The request for the SAML token is secured with the eID[1] of the doctor. The certificate used by the Holder-Of-Key (HOK) verification mechanism is an eHealth certificate.

The needed attributes are the following :

- The social security identification number of the physician:
    - *urn:be:fgov:person:ssin*
    - *urn:be:fgov:ehealth:1.0:certificateholder:person:ssin*

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

- The social security identifier number of the doctor :

---

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

- o ***urn:be:fgov:person:ssin***

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

- To have access to the Chapter 4 Consult web service, the person must be a physician having valid visa and NIHII number :

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

2.2 Pharmacist in a pharmacy

Warning: Access is only allowed to Chapter IV consultation. Pharmacies do not have access to the Chapter IV Admission service.

Pharmacies must specify several attributes in the request. The request to the STS is secured with the eID[2] of the pharmacist starting the session. The certificate of the pharmacy issued by eHealth is used by the HOK mechanism.

The attributes that need to be provided in the request are the following :

- The social security identifier number of the person starting the session (the person must be a recognized pharmacist):

  - o ***urn:be:fgov:person:ssin***

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

- The identifier of the pharmacy:

  - o ***urn:be:fgov:ehealth:1.0:pharmacy:nihii-number***

- The identifier of the pharmacy holder:

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

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

- The SSIN of the person (must be a pharmacist) starting the session, this is verified by eHealth :

  - o ***urn:be:fgov:person:ssin***

  - o ***urn:be:fgov:ehealth:1.0:certificateholder: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 :

  - o ***urn:be:fgov:ehealth:1.0:pharmacy:nihii-number***

- The identifier of the pharmacy holder (SSIN), i.e. the pharmacist responsible for all activities performed in the pharmacy :

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

- The identifier of the pharmacy holder (NIHII11), i.e. the pharmacist responsible for all activities performed in the pharmacy :

  - o ***urn:be:fgov:person:ssin:ehealth:1.0:pharmacy-holder:certified:nihii11***

- The pharmacy must be a recognised pharmacy :

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

- The pharmacy holder must be the certified pharmacy holder of the given pharmacy :

---

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

- - *urn:be:fgov:ehealth:1.0:pharmacy:nihii-number:person:ssin:ehealth:1.0:pharmacy-holder:boolean*
- The person must be a recognized pharmacist :
  - *urn:be:fgov:person:ssin:ehealth:1.0:fpsph:pharmacist:boolean*

2.3 Healthcare institution

2.3.1 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 :

- 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 :
  - *urn:be:fgov:ehealth:1.0:hospital:nihii-number*
  - *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number*
- The hospital must be a recognized hospital :
  - *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number:recognisedhospital:boolean*
- The NIHII number(11 positions) of the hospital :
  - *urn:be:fgov:ehealth:1.0:hospital:nihii-number:recognisedhospital:nihii11*