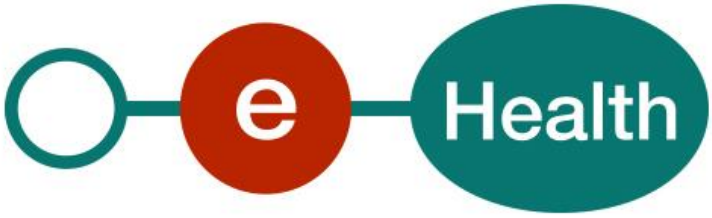

Global Medical File - MCN
SSO

eHealth platform

Willebroekkaai 38 – 1000 Brussel

38, Quai de Willebroeck – 1000 Bruxelles

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.	20/04/2016	eHealth platform	Initial version
1.1	15/02/2017	eHealth platform	Footnote complement
1.2	04/09/2018	eHealth platform	Update

2. Use of the eHealth SSO solution

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

To access to the MyCareNet Tarification 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 platform to verify that the requested test cases were correctly configured.

See the documents GMD_STS_samlRequest.xml and GMD_STS_samlResponse.xml provide STS request/response examples on the portal of the eHealth platform.

For the GMF services, we differentiate between two types of doctors: general practitioners and specialists (either as individual or within a hospital). Note that the access rules for the doctor (as individual or within a hospital) are slightly different for the two services: notification of the GMF service and the consultation of the GMF service. More in particular:

- Consultation service: this service is accessible by dentist and both types of doctors (general practitioners and specialists)
- Notification service: this service is accessible only by the general practitioners, specialists do not have access to this service

Nevertheless, both types of doctors use the same type of token (we do not differentiate between the two types of doctors on the SAML token level). In order to facilitate the Single Sign On the SAML tokens as described in this section (doctor as individual and doctor within a hospital) are the same as for some other services used by the two types of doctors (e.g., Chapter IV), where we do not differentiate between the two types of doctors. The particular access rules (service accessible only by general practitioners or service accessible by both; general practitioners and specialists) are then enforced by the eHealth platform at the reception of the request.

2.1 Doctor as individual

The request for the SAML token is secured with the eID of the doctor[1]. 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 doctor: urn:be:fgov:ehealth:1.0:certificateholder:person:ssin and urn:be:fgov:person:ssin

Doctors must also specify which information must be asserted by the eHealth platform:

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

[1] *As fallback, in absence of the eID, the personal eHealth certificate can be used for authentication instead.*
A "fallback session" is exceptional and temporary. In case of unavailability of the eID of the healthcare professional, in order to safeguard business continuity of the healthcare professional- temporarily an alternative fallback mechanism with manual entry of the password of the eHealth keystore (certificate) may be chosen. Systematical, repeated use of this method is not allowed.

- The NIHII number of the doctor (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:person:ssin:ehealth:1.0:doctor:nihii11
- The doctor must be a general practitionner (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:person:ssin:ehealth:1.0:nihii:doctor:generalist:boolean

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 needed 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 and urn:be:fgov:ehealth:1.0:hospital:nihii-number

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

- 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 and 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 NIHII number (11 positions) of the hospital (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:ehealth:1.0:hospital:nihii-number:recognisedhospital:nihii11
- The doctor must be a general practitionner (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:person:ssin:ehealth:1.0:nihii:doctor:generalist:boolean
- 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 Dentist as individual

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

Dentists must also specify which information must be asserted by the eHealth platform:

- The social security identification number of the dentist: (AttributeNamespace: "urn:be:fgov:identification-namespace") urn:be:fgov:ehealth:1.0:certificateholder:person:ssin and 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 NIHII number of the dentist (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:person:ssin:ehealth:1.0:nihii:dentist:nihii11

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