



**MyCareNet - Global Medical File  
SSO  
v1.3**

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

**eHealth platform**

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

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

# Table of contents

Table of contents .....	2
1. Document management .....	3
1.1 Document history .....	3
2. Use of the eHealth SSO solution .....	4
2.1 Doctor as individual .....	4
2.2 Doctor within a hospital.....	4
2.3 Dentist as individual.....	5

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
1.3	30/01/2023	eHealth platform	Update doctor attributes

## 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 GlobalMedicalFile 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.

For the GMF services, access rules for the doctor (as individual or within a hospital) or the dentist are slightly different for the two services:

- Consultation service: this service is accessible by the dentists and by the doctors (as individual or within a hospital)
- Notification service: this service is accessible only by the doctors (as individual or within a hospital)

### 2.1 Doctor as individual

The request for the SAML token is secured with the eID of the doctor<sup>1</sup>. 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 NIHII number of the doctor (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:person:ssin:ehealth:1.0:doctor: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 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

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

---

<sup>1</sup> As fall-back, in absence of the eID, the personal eHealth certificate can be used for authentication instead.

A “fall-back 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 fall-back mechanism with manual entry of the password of the eHealth keystore (certificate) may be chosen. Systematical and repeated use of this method is not allowed.

- The social security identification number of the doctor (AttributeNamespace: "urn:be:fgov:identification-namespace"): urn:be:fgov:person:ssin
- The NIHI number of the hospital: urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihi-number and urn:be:fgov:ehealth:1.0:hospital:nihi-number
- The NIHI number of the doctor (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:person:ssin:ehealth:1.0:doctor:nihi11
- The NIHI number (11 positions) of the hospital (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:ehealth:1.0:hospital:nihi-number:recognisedhospital:nihi11
- The hospital must be a recognized hospital (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth") :
- urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihi-number:recognisedhospital:boolean

## 2.3 Dentist as individual

The request for the SAML token is secured with the eID<sup>2</sup> 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 NIHI number of the dentist (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth"): urn:be:fgov:person:ssin:ehealth:1.0:nihi:dentist:nihi11

---

<sup>2</sup> As fall-back, only in absence of the eID, the personal eHealth certificate can be used for authentication instead.