How to call the Chapter IV web services and the test process
Cookbook
Version 1.03

This document is provided to you free of charge by the

eHealth platform

Willebroekkaai 38

38, Quai de Willebroek

1000 BRUSSELS

Table of contents

To the attention of: “IT expert” willing to integrate the Chapter IV web services.

1. Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1	24/05/2011	eHealth platform	First version
1.01	1/12/2011	eHealth platform	Updated
1.02	16/01/2015	eHealth platform	Update hyperlinks in French and Dutch
1.03	19/12/2019	eHealth platform	ETK - Additional information

2. Introduction

2.1 Goal of the service

The eHealth platform makes available to the medical advisors of the healthcare insurance organization and the caregivers dedicated services to the medical agreements 'Chapter IV' precisely:

- The demand for the medical advisor agreements.
- The consultation of the medical advisor agreements.

2.2 Goal of the document

This document describes how to test the Chapter IV web service.

2.3 eHealth platform - document references

All the document references can be found on the eHealth portal[1].

ID	Title	Version	Date	Author
1	Glossary		DD/MM/YYYY	eHealth platform
2	MyCareNet – Chapter IV functional description			
3	STS Cookbook	1.3	18/07/2018	eHealth platform
4	Connectors	3.4	07/04/2015	eHealth platform
5	ETEE		18/07/2018	eHealth platform

[1] ***https://www.ehealth.fgov.be/ehealthplatform***

3. Support

3.1 For issues in production

eHealth platform contact center:

- Phone: 02/788 51 55
- Mail: ***support@ehealth.fgov.be***
- *Contact Form :*
  - ***https://www.ehealth.fgov.be/ehealthplatform/nl/contact*** (Dutch)
  - ***https://www.ehealth.fgov.be/ehealthplatform/fr/contact*** (French)

3.2 For issues in acceptance

Integration-support@ehealth.fgov.be

3.3 For business issues

- regarding an existing project: the project manager in charge of the application or service
- regarding a new project and other business issues: ***info@ehealth.fgov.be***

3.4 Certificates

- In order to access the secured eHealth platform environment you have to obtain an eHealth platform certificate, used to identify the initiator of the request. In case you do not have one please consult the chapter about the eHealth Certificates on the portal of the eHealth platform

  https://www.ehealth.fgov.be/ehealthplatform/nl/ehealth-certificaten

  https://www.ehealth.fgov.be/ehealthplatform/fr/certificats-ehealth
- For technical issues regarding eHealth platform certificates

  Acceptance: ***acceptance-certificates@ehealth.fgov.be***

  Production: ***support@ehealth.fgov.be***

4. Step-by-step

4.1 Requirements

In order to be able to test the Chapter IV services, you need to take the following steps:

1. **Create test cases (test users):** You always need to request the configuration of the test cases at the eHealth platform. The administrative steps that need to be taken and the form that must be filled out can be found in the documentation provided by MyCareNet (CIN/NIC) (see "MyCareNet functional description 01.zip" archive).
2. **Request an eHealth test certificate:** test certificates must be requested at the eHealth platform. Nevertheless, the previously obtained eHealth test-certificates can be also used.
3. **Obtain the SAML token from the STS:** the Belgian eID is used for identification at the STS and the certificate obtained in the previous step is used as a Holder-Of-Key certificate.
4. **Call the web services with an already encrypted test message:** an example encrypted message can be found in the documentation provided by MyCareNet (CIN/NIC) (see the documentation contained in the "MyCareNet functional description 01.zip" archive).
5. **Implement the encryption of the message:** you need to implement retrieving an ETK from the ETK depot and using it to encrypt the message before sending it.
6. **Call the web services including the encryption process**.

4.2 Create test cases

The rules to access the Chapter IV web services are the same in test as in production.

Access rules:

- authentication with an eID of the user (or personal eHealth certificate as fallback)
- the access rules for the particular services and the information that needs to be contained in the SAML token can be found in the **"Chapter IV service specification"**.

All test cases have to be configured by the development team of the eHealth platform.
Before doing any tests, request your test cases from the eHealth (***info@ehealth.fgov.be***).

4.3 Request test certificates

Prior to requesting the certificate, you need the latest versions of *Java 1.6* and the *Belgium eID middleware*.
You also need a smart-card reader and a Belgian eID. You can request the test certificate at the following URLs:

http://wwwacc.ehealth.fgov.be/JWS/ETEE/etee-requestor_fr.jnlp (French version)

http://wwwacc.ehealth.fgov.be/JWS/ETEE/etee-requestor_nl.jnlp (Dutch version)

You will need NIHII and CBE identification numbers (obtained in the previous step) of the test pharmacy in order to request the certificate.

4.4 Obtain SAML token

The usage of the eHealth Secure Token Service (STS) and the structure of the exchanged xml-messages are described in the eHealth STS cookbook (See section 2.4)

In order to implement a call to the eHealth STS you can reuse the implementation as provided in the "eHealth technical connector" (see section 2.4)

Nevertheless, eHealth implementations use standards and any other compatible technology (web service stack for the client implementation) can be used instead.

The attributes that need to be provided and the attributes that should be certified by the eHealth platform in order to obtain a token valid for Chapter IV services are described in section 2 of **"Chapter IV service specification"**.

To access the Chapter IV web services, the response token must contain “true” for all of the certification attributes. If you obtain “false”, contact the eHealth platform to verify that the requested test cases were correctly configured.

4.5 Call the Chapter IV service using an already encrypted message

To do the first call to one of the Chapter IV web services:

- Use the example messages (with already encrypted parts) (see the documentation contained in the "MyCareNet functional description 01.zip" archive). and place them in the SOAP body
- Add the SAML Token, timestamp and the signature to the SOAP header

In order to implement a web service call protected with a SAML token you can reuse the implementation as provided in the "eHealth technical connector". Nevertheless, eHealth implementations use standards and any other compatible technology (web service stack for the client implementation) can be used instead.

If your call is successful, you will receive valid business response.

4.6 Call the Chapter IV service using encryption

All the information about the use of the encryption libraries and the call to the ETK (eHealth Token Key) depot are described in the End-To-End Encryption (ETEE) cookbooks (see section 2.4)

To encrypt the request parts, you have to call the GetEtk operation to pick up the right ETK from the eHealth ETK depot. The table below provides you the identifiers to use in the GetEtkRequest.

Environment	Type	Value	Application ID
Integration Test Environment	CBE	0820563481	MYCARENET
Acceptance Environment	CBE	0820563481	MYCARENET
Production Environment	CBE	0820563481	MYCARENET

The encryption to a HIO (unknown recipient encryption) is done with a symmetric key as obtained from the KGSS. In order to allow any HIO (but only a HIO) to decrypt the message, the key has to be requested with the allowed-reader specified with the following arguments:

- **Namespace:** urn:be:fgov:certified-namespace:ehealth
- **Name:** urn:be:fgov:kbo-bce:organization:cbe-number:ehealth:1.0:hio:boolean
- **Value:** true

For example:

```
<GetNewKeyRequestContent xmlns="urn:be:fgov:ehealth:etee:kgss:1_0:protocol">
        <AllowedReader>
                <Namespace>urn:be:fgov:certified-namespace:ehealth</Namespace>
                <Name>urn:be:fgov:kbo-bce:organization:cbe-number:ehealth:1.0:hio:boolean</Name>
                <Value>true</Value>
        </AllowedReader>
        <ETK>MIAGCS...</ETK>
</GetNewKeyRequestContent>
```

Remark:

The ETK of the KGSS should be retrieved using the ETKDepot[2] WS.

The following search criteria must be given to request the ETK of the KGSS:

- Type: CBE
- Value: 0809394427
- ApplicationId: KGSS

4.7 Call the Chapter IV service

To call to one of the Chapter IV web services:

- Prepare the message (encrypt, etc.) and add it to the SOAP body
- Add the SAML Token, timestamp and the signature to the SOAP header

In order to implement a web service call protected with a SAML token you can reuse the implementation as provided in the "eHealth technical connector". Nevertheless, eHealth implementations use standards and any other compatible technology (web service stack for the client implementation) can be used instead.

If your call is successful, you will receive a valid business response.

If you receive an error, it could be caused by an error in your request. If you do not find any error in your request:

- If it is a soap exception, contact the eHealth platform team to receive more information about the occurred error. (See Chap 3)
- If it is a business error, contact ***servicedesk@mycarenet.be***

The soap header (only when the received response is not a SOAP fault) contains a message ID, e.g.:

<soapenv:Header>

<add:MessageID xmlns:add="http://www.w3.org/2005/08/addressing">**6f23cd40-09d2-4d86-b674-b311f6bdf4a3**</add:MessageID>

</soapenv:Header>

This message ID is important for tracking of the errors and it should be provided (when available) when requesting support.

[2] *See referenced document: "Cookbook v.2.0: End-to-end Encryption for a known recipient (addressed messages)"*

5. Examples

Please refer to the documentation provided by MyCareNet (CIN/NIC) (see "MyCareNet functional description 01.zip" archive).