How to call the Qermid TuCo web services and the test process
Cookbook
Version 1.2

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

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
1.0	06/02/2012	eHealth platform	Initial version
1.1	22/03/2019	eHealth platform	New application ID for the encryption of the KMEHR content
1.2	04/08/2022	eHealth platform	§ 3 Support (updated) § 4.7 WS-I Basic Profile (added) § 4.8 Tracing (added)

2. Introduction

2.1 Goal of the service

pm

2.2 Goal of the document

This document describes how to test the Qermid TuCo web service (WS).

In order to be able to test the Qermid TuCo services, you need to take the following steps (see also section 3):

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 Qermid (see the documentation contained in the "Qermid_Tuco web service.zip" archive).
2) Request an eHealth test certificate: test certificates must be requested at the eHealth platform. Nevertheless, you might reuse the previously obtained eHealth test-certificates (see link below and the document references in this document).

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

   https://www.ehealth.fgov.be/ehealthplatform/fr/certificats-ehealth
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 (HOK) certificate.
4) Call the web services with an already encrypted test message: an example encrypted message can be found in the documentation provided by Qermid (see the documentation contained in the "Qermid_Tuco web service.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. This document is not a development or programming guide for internal applications. Instead, it provides functional and technical information and allows an organization to integrate and use the eHealth platform service.

However, in order to interact in a smooth, homogeneous and risk controlled way with a maximum of partners, these partners must commit to comply with the requirements of specifications, data format and release processes of the eHealth platform as described in this document.

Technical and business requirements must be met in order to allow the integration and validation of the eHealth platform service in the client application.

2.3 eHealth platform document references

On the portal of the eHealth platform, you can find all the referenced documents.[1]. These versions or any following versions can be used for the eHealth platform service.

ID	Title	Version	Description
1	Glossary	pm	Pm
2	Qermid_Tuco web service.zip	0.1	Functional documentation provided by Qermid. Describes the structure of the exchanged messages, functional description of the XML elements etc.

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

3	SSO eHealth Qermid TuCo	1.1	Technical description of the Qermid TuCo WS

3. Support

3.1 Helpdesk eHealth platform

3.1.1 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***

3.1.2 For issues in production

eHealth platform contact centre:

- Phone: 02 788 51 55 (on working days from 7 am till 8 pm)
- 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)

3.1.3 For issues in acceptance

Integration-support@ehealth.fgov.be

3.1.4 For business issues

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

3.2 Status

The website ***https://status.ehealth.fgov.be*** is the monitoring and information tool for the ICT functioning of the eHealth services that are partners of the Belgian eHealth system.

4. Step-by-step

4.1 Create test cases

The rules to access the Qermid Tuco web services are the same in test as in production. Access rules:

- authentication with an hospital eHealth certificate
- the access rules for the particular services and the information that needs to be contained in the SAML token can be found in the "Qermid Tuco service specification".

4.2 Request test certificates

Before doing any tests, request your test cases at info@ehealth.fgov.be

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 URL:

http://wwwacc.ehealth.fgov.be/JWS/ETEE/etee-requestor_fr.jnlp

http://wwwacc.ehealth.fgov.be/JWS/ETEE/etee-requestor_nl.jnlp

You will need a NIHII identification number of the test hospital in order to request the certificate.

4.3 Obtain SAML Token

The usage of the eHealth Secure Token Service and the structure of the exchanged xml-messages are described in the eHealth STS cookbook.

In order to implement a call to the eHealth STS you can reuse the implementation as provided in the "eHealth technical connector" on the portal of the eHealth platform.

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 eHealth in order to obtain a token valid for Qermid Tuco services are described in section 2 of "Service specification eHealth- Qermid_Tuco".

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

4.4 Call the Qermid TuCo service using an already encrypted message

To do the first call to one of the Qermid Tuco web services:

- Use the example messages (with already encrypted parts) and place them in the SOAP body
- Add the SAML Token, timestamp and the signature to the SOAP header

In order to implement a webservice 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.

4.5 Call the Qermid TuCo 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 on the portal of the eHealth platform.

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
Acceptation environment	CBE	0206653946	ECAREAPPACC
Production environment	CBE	0206653946	ECAREAPPPRD

For more information: see the documentatioin in the Qermid TuCo WS zip archive

4.6 Call the Qermid TuCo service

To call to one of the Qermid Tuco 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 webservice 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 might be caused by an error in your request.

If it is a soap exception, contact the eHealth team (***support@ehealth.fgov.be***) to receive more information about the occurred error.

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. It should be provided (when available) when requesting support.

4.7 WS-I Basic Profile 1.1

Your request must be WS-I compliant (See Chap 2.4 - External Document Ref).

4.8 Tracing

To use this service, the request SHOULD contain the following two http header values (see RFC ***https://datatracker.ietf.org/doc/html/rfc7231#section-5.5.3***):

1. User-Agent: information identifying the software product and underlying technical stack/platform. It MUST include the minimal identification information of the software such that the emergency contact (see below) can uniquely identify the component.
   a. Pattern: {minimal software information}/{version} {minimal connector information}/{connector-package-version}

b. Regular expression for each subset (separated by a space) of the pattern: [[a-zA-Z0-9-\/]*\/[0-9azA-Z-_.]*

c. Examples:
User-Agent: myProduct/62.310.4 Technical/3.19.0
User-Agent: Topaz-XXXX/123.23.X freeconnector/XXXXX.XXX

2. From: email-address that can be used for emergency contact in case of an operational problem.
Examples:

From: ***info@mycompany.be***

5. Examples

See the documentation provided by Qermid in the Qermid_Tuco webservice.zip archive