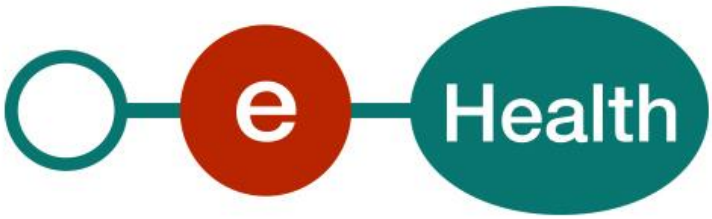


eCare Orthopride WS
Cookbook
Version 1.2

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	11/12/2014	eHealth platform	Initial version
1.1	19/07/2018	eHealth platform	Update
1.2	22/03/2019	eHealth platform	New application ID for the encryption of the KMEHR content

2. Introduction

2.1 Goal of the service

The Orthopride web service (WS) allows surgeons authorized to place or remove orthopaedic implants to register hip and knee prosthesis through a dedicated hospital system.

2.2 Goal of the document

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 service.

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

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

2.3 eHealth document references

All the document references can be found on the portal of the eHealth platform[1]. These versions or any following versions can be used for the eHealth service.

ID	Title	Version	Date	Author
1	Glossary.pdf		pm	eHealth platform
2	eHealth STS	1.2	12/04/2018	eHealth platform
3	Cookbook End-to-End vercijfering – Bekende bestemmeling/Système de cryptage End-to-End Destinataire connu	2.4	18/07/2018	eHealth platform

2.4 External document references

All documents can be found through the internet. They are available to the public, but not supported by the eHealth platform.

ID	Title	Source	Date	Author
1	OASIS SAML Token Profile	***http://www.oasis-open.org/committees/download.php/16768/wssv1.1-spec-os-SAMLTokenProfile.pdf***	01/02/2006	OASIS

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

3. Business and privacy requirements

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***

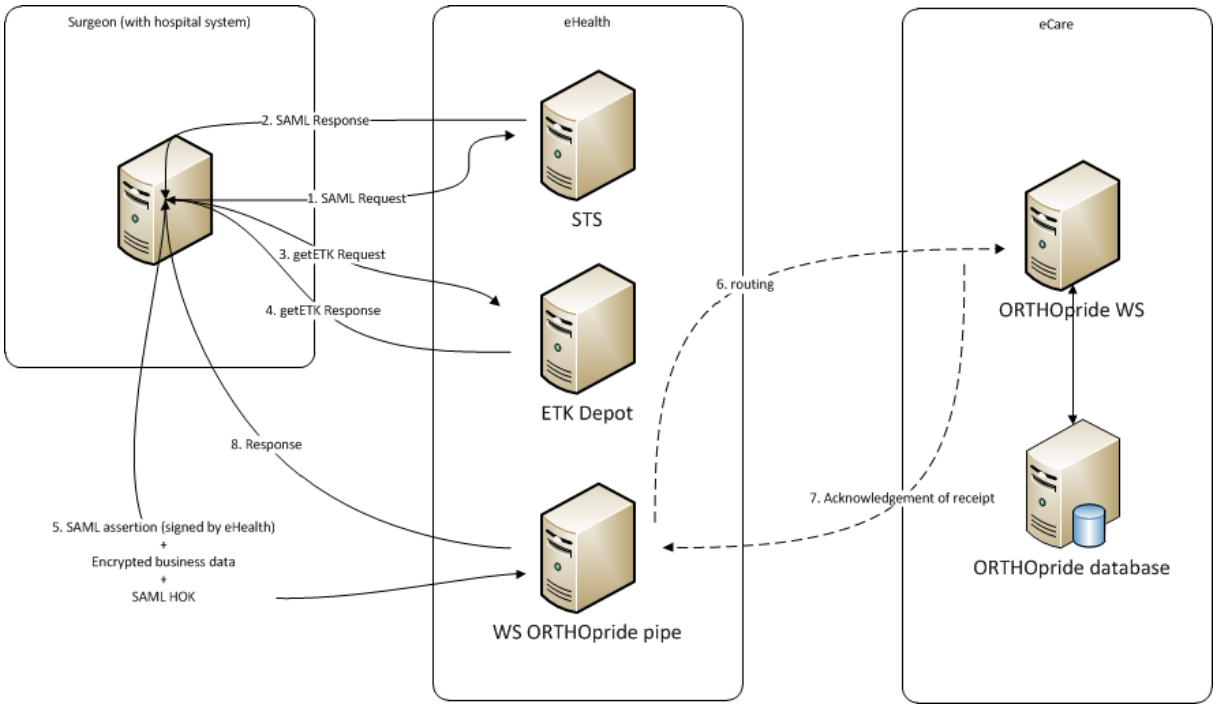
  Production: ***support@ehealth.fgov.be***

  info@ehealth.fgov.be

3.5 eCare contact

For questions about the business content of the message, please contact: ***ecare-help@smals.be***

4. Global overview



The first step is to request a SAML token from our STS service. See 5.1.1 for more details. After receiving a valid token, an eHealth Token Key (ETK) is needed for the encryption of the business message. This ETK is retrieved from our ETK depot. See 5.1.2 for more details.

The next step is to create the business message (see the cookbook provided by eCare inside “eCare ORTHOpride WS.zip”), encrypt it using the ETK and calling the WS ORTHOpride pipe. This request and the response are described in **Error! Reference source not found.**.

5. Step-by-step

5.1 Technical requirements

5.1.1 Use of the eHealth SSO solution

The complete overview of the profile and a systematic implementation to start protecting a new application with SSO @ eHealth is 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":

- ***https://www.ehealth.fgov.be/ehealthplatform/nl/service-ehealth-platform-services-connectors***
- ***https://www.ehealth.fgov.be/ehealthplatform/fr/service-ehealth-platform-services-connectors***

Nevertheless, eHealth implementations use standards and any other compatible technology (WS 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 eCare Orthopride services are described in sections 5.1.1.1 and 5.1.1.2. To access the eCare Orthopride WS, 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.

5.1.1.1 Orthopedist within a 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 (AttributeNamespace: "urn:be:fgov:identification-namespace"):

- The social security identification number of the orthopedist: *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*

You 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 (AttributeNamespace: "urn:be:fgov:identification-namespace"): *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number* and *urn:be:fgov:ehealth:1.0:hospital:nihii-number*
- the hospital must be a recognized hospital (AttributeNamespace: *urn:be:fgov:certifiednamespace:ehealth*) *urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number:recognisedhospital:boolean*

Additionally, the eHealth platform will use the social security identification number, as certified by the eHealth platform, to verify the NIHII number of the person and to verify that the person is a recognized orthopaedist.

5.1.1.2 Surgeon within a hospital

The SAML token is the same as discussed above, but additionally the eHealth platform will use the social security identification number, as certified by the eHealth platform, to verify the NIHII number of the person and to verify that the person is a recognized surgeon.

5.1.2 Encryption

The business part of the message to send to the web service must be encrypted.

To encrypt the message, you should retrieve the public key on the ETK depot. Then, encrypt the message using this public key via eHealth encryption libraries.

All the information about the use of the encryption libraries and the call to the ETK depot are described in the cookbooks available the eHealth website ("Cookbook ETEE Bekende bestemmeling"/"Cookbook ETEE Destinataire connu"). The table below provides you with the identifiers to use in the GetEtkRequest.

Environment	Type	Value	Application ID
Acceptance Environment	CBE	0206653946	**ECAREAPPACC**
Production Environment	CBE	0206653946	**ECAREAPPPRD**

More information can be found in the cookbook documents provided by eCare (contained in the "eCare Orthopride WS.zip" archive).

5.1.3 Security policies to apply

We expect that you use SSL one way for the transport layer.

As WS security policy, we expect:

- A timestamp (the date of the request), with a Time to live of one minute (if the message does not arrive during this minute, it shall not be treated).
- The signature with the certificate of
  - the timestamp, (the one mentioned above)
  - the body (the message itself)
  - and the binary security token: a SAML token issued by STS

  This will allow eHealth to verify the integrity of the message and the identity of the message author.

A document explaining how to implement this security policy can be obtained at the eHealth platform.

The STS cookbook can be found on the portal of the eHealth platform.

5.2 Process overview

Summary:

To call the eCare Orthopride WS:

- Add the encrypted business message to the *SendCMSMessageRequest* element (base64). See section 5.3.
- Add to the SOAP header the following elements:
  - **SAML Token**: The SAML Assertion received from the eHealth STS. This Assertion needs to be forwarded exactly as received in order to not to break the signature of the eHealth STS. The token needs to be added accordingly to the specifications of the OASIS SAML Token Profile (holder-of-key).
  - **Timestamp**.
  - A **signature** that has been placed on the SOAPBody with the certificate of which the public key is mentioned in the SAML Assertion.
- The signature element (mentioned above) needs to contain:
  - SignedInfo with References to the soapBody.
  - KeyInfo with a SecurityTokenReference pointing to the SAML Assertion.

See also the WSSP in the WSDL[2].

As for now, only the operations described below are available. The operations for the WS are:

- sendEcareDeclaration
- updateEcareDeclaration
- deleteEcareDeclaration

The endpoints and service contract (ehealth XSDs) for each of these operations can be found in the Registry on the eHealth portal.

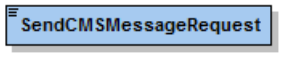
For more details, see the cookbook documents as provided by eCare (contained in the "eCare Orthopride WS.zip" archive).

5.3 Web service

5.3.1 sendCMSMessage

This method is used to send the encrypted eCare business message to the eCare platform through the eHealth platform.

5.3.1.1 Request



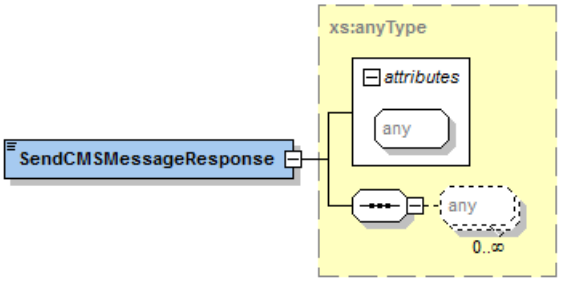
The input request is defined by a tag, which will contain the encrypted request in base64. For more details, see the cookbook documents as provided by eCare (contained in the "eCare Orthopride WS.zip" archive).

5.3.1.2 Response

There are different possible types of response:

If there are no technical errors, responses as described in the remainder of this section are returned.
In case of a technical error: see chapter 8.

For more details on the specific elements and the concepts behind them, see the cookbook documents as provided by eCare (contained in the "eCare Orthopride WS.zip" archive).



The output response is defined by a tag, which will contain the encrypted response provided by the eCare Orthopride WS. For more details and how to decrypt, see the *cookbook* documents as provided by eCare (contained in the "eCare Orthopride WS.zip" archive).

---

[2] *WSDL's can be found in the eHealth Service Registry:* ***https://services.ehealth.fgov.be/registry/uddi/bsc/web*** *or* ***https://services-acpt.ehealth.fgov.be/registry/uddi/bsc/web*** *for services in the acceptance environment*.

6. Risks and security

6.1 Security

6.1.1 Business security

In case the development adds an additional use case based on an existing integration, the eHealth platform must be informed at least one month in advance with a detailed estimate of the expected load. This will ensure an effective capacity management.

In case of technical issues on the WS, the partner may obtain support from the contact center.

In case the eHealth platform finds a bug or vulnerability in its software, the partner is advised to update his application with the newest version of the software within 10 business days.

In case the partner finds a bug or vulnerability in the software or web service that the eHealth platform delivered, he is obliged to contact and inform the eHealth platform immediately and he is not allowed to publish this bug or vulnerability in any case.

6.1.2 Web service

WS security used in this manner is in accordance with the common standards. Your call will provide:

- SSL one way
- Time-to-live of the message: one minute.
- Signature of the timestamp, body and binary security token. This will allow the eHealth platform to verify the integrity of the message and the identity of the message author.
- No encryption on the message (only the business part is encrypted).

7. Test procedure

This chapter explains the procedures for testing Orthopride WS in acceptation or production.

7.1 Request a test case

To be authorized to call the WS, the hospital must be configured in the eHealth acceptance environment. So, fill out the excel file that is contained in the "Ecare_ Orthopride web services.zip" archive and send it to ***info@ehealth.fgov.be***

After the configuration is done, a certificate should be requested for this hospital.

7.2 Request a hospital certificate

The developed functionality needs to be tested using an acceptance certificate for hospital. Therefore, a participating test-hospital must first have a certificate-responsible because a hospital-acceptance test is required to perform the necessary acceptance tests on-site (in a pilot hospital). Software companies may only conduct acceptance tests in the acceptance environment of the hospital where the acceptance certificate and key pair of the specific environment shall be consulted on the predefined path (“Home Directory” under: \ehealth\keystore\ as set out in eHealth Certificate Manager – manual § 2.1.12).

8. Error and failure messages

There are different possible types of response:

- If there are no technical errors, responses as described in section 5.3 are returned.
- In the case of a technical error, a SOAP fault exception is returned (see table below)

If an error occurs, first please verify your request. Following table contains a list of common system error codes for the eHealth Service Bus.

Description of the possible SOAP fault exceptions.

Error code	Component	Description	Solution/Explanation
SOA-00001	Unknown	Service error	This is the default error sent to the consumer in case no more details are known.
SOA-01001	Consumer	Service call not authenticated	From the security information provided, • or the consumer could not be identified • or the credentials provided are not correct
SOA-01002	Consumer	Service call not authorized	• The consumer is identified and authenticated, but is not allowed to call the given service.
SOA-02001	Provider	Service not available. Please contact service desk	• An unexpected error has occurred • Retries will not work • Service desk may help with root cause analysis
SOA-02002	Provider	Service temporarily not available. Please try later	• An unexpected error has occurred • Retries should work • If the problem persists service desk may help
SOA-03001	Consumer	Malformed message	This is a default error for content related errors in case no more details are known.
SOA-03002	Consumer	Message must be SOAP	Message does not respect the SOAP standard
SOA-03003	Consumer	Message must contain SOAP body	Message respects the SOAP standard, but body is missing
SOA-03004	Consumer	WS-I compliance failure	Message does not respect the WS-I standard
SOA-03005	Consumer	WSDL compliance failure	Message is not compliant with WSDL in Registry/Repository
SOA-03006	Consumer	XSD compliance failure	Message is not compliant with XSD in Registry/Repository
SOA-03007	Consumer	Message content validation failure	From the message content (conform XSD): • Extended checks on the element format failed • Cross-checks between fields failed