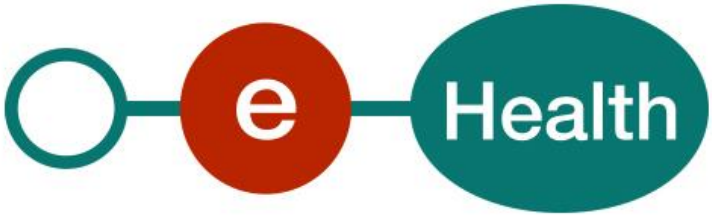


eAttest Web Service
Cookbook
Version 1.3

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	29/11/2016	eHealth platform	First version
1.1	06/02/2017	eHealth platform	Draft WS eAttest for review
1.2	07/04/2016	eHealth platform	Added attribute “ContentEncryption” in Detail element
1.3	17/09/2018	eHealth platform	Update

2 Introduction

2.1 Goal of the service

The eAttest Web Service (WS) allows the care providers to send a healthcare provided certificate electronically to the insurance institutions. The care provider needs to request a SAML token from the eHealth Secure Token Service (STS) prior to calling the Generic Insurability services.

2.2 Goal of the document

This document is not a development or a 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.

Detailed description of the functionality of the service, the semantics of the particular elements and other general information about the service is out of the scope of this document. This kind of information can be found in the documentation provided by MyCareNet on their Sharepoint.

In order to be able to test the MyCareNet eAttest service, you need to take the following steps (see also section 5):

1. **Create a test case:** If the testing is done for a real care provider, the real NIHII number of the care provider can be used. Otherwise, you will receive a test NIHII number from the eHealth development team (you must indicate the service called and the kind of profile needed). You always need to request the configuration of the test cases at eHealth.
2. **Request an eHealth test certificate:** a test certificate must be requested at the eHealth platform.
3. **Obtain the SAML token from the STS:** the eHealth test certificate obtained in the previous step is used for identification at the STS and as the Holder-Of-Key (HOK) certificate.
4. **Call the eAttest web services**.

2.3 eHealth document references

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

ID	Title	Version	Date	Author
1	Glossary.pdf	1.0	01/01/2010	eHealth platform
2	Cookbook STS	1.2	13/04/2018	eHealth platform
3	eAttest_SSO.pdf	1.1	17/09/2018	eHealth platform

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

2.4 External document references

All the MyCareNet documentation can be found within their Sharepoint[2]. The documentation referenced in this section may evolve in time.

If some external documentation has been modified, please notify the eHealth service management[3] who manages the maintenance of this document.

ID	Title	Version	Last modification date	Author
1.	Web Service Security – SAML Token profile 1.1 ***http://www.oasis-open.org/committees/download.php/16768/wssv1.1-spec-os-SAMLTokenProfile.pdf***	NA	01/02/2006	OASIS
2.	GenericSync Error codes	NA	08/02/2017	CIN
3.	ImplementationGuide_For_CareProvider	NA	08/02/2017	CIN
4.	Messages definition NIPPIN eAttest v1	NA	21/03/2017	CIN
5.	MyCareNet Authentication Catalogue	NA	08/02/2017	CIN
6.	NIPPIN GenSync (ESB 2 NIPPIN)	NA	10/03/2017	CIN
7.	Service_Catalogue_Commons	NA	10/03/2017	CIN
8.	Service_Catalogue_GenSync	NA	15/03/2017	CIN
9.	Codes erreurs-bijlage Verwerpingscodes – CI 20161025	NA	02/03/2017	CIN
10.	Cross check eAttest v1	NA	08/02/2017	CIN
11.	Description fonctionnelle des services – eAttest – FR – V1.0	NA	08/02/2017	CIN
12.	Functionele beschrijving van de diensten – eAttest – NL – V1.0	NA	08/02/2017	CIN
13.	Kmehr – Annexe HCPARTY – FR – V01r04	NA	08/02/2017	CIN
14.	Kmehr – Bijlage HCPARTY – NL – V01r04	NA	08/02/2017	CIN
15.	Kmehr – eAttest – FR – V02R00 CA	NA	15/03/2017	CIN
16.	Kmehr – eAttest – NL – V02R00 CA	NA	15/03/2017	CIN
17.	Kmehr – Protocol eHealth message service – NL – V01r04	NA	08/02/2017	CIN
18.	Kmehr – Protocole eHealth message service – FR – V01r04	NA	08/02/2017	CIN

[2] In order to have access to the Sharepoint, you need to create an account which can be requested at : ***http://fra.mycarenet.be/wie-zijn-we/contact or http://ned.mycarenet.be/wie-zijn-we/contact***

[3] ***ehealth_service_management@ehealth.fgov.be***

19.	xsd-kmehr message protocole-1_18	NA	08/02/2017	CIN
20.	xsd-encryption	NA	15/03/2017	CIN

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***

3.5 Support desk CIN/NIC - contact points

3.5.1 eAttest business support

For business questions related to eAttest: MyCareNet Helpdesk (first line support)

3.5.2 MyCareNet Helpdesk:

Telephone: 02/891 72 00

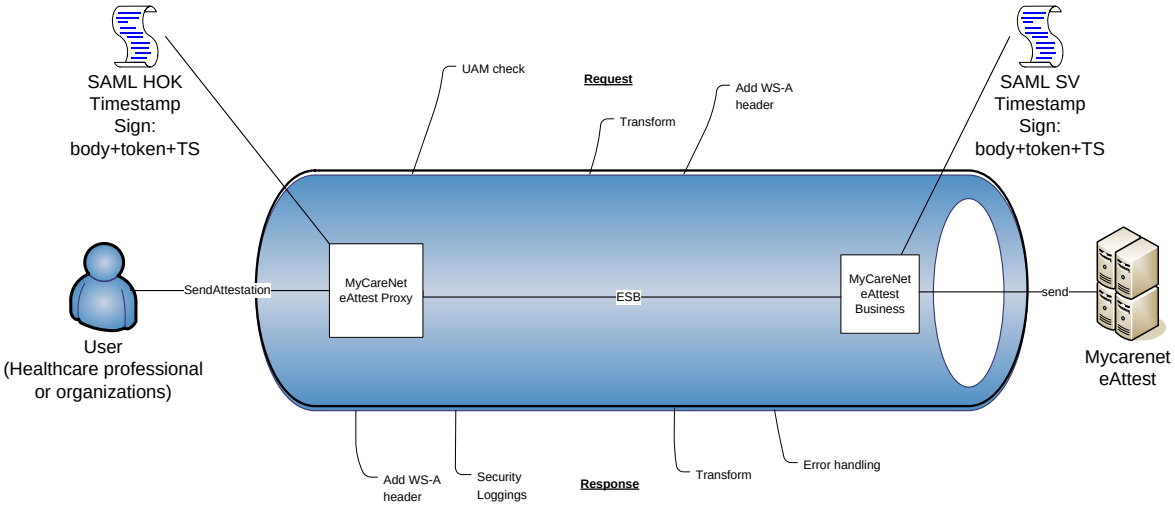
Mail: ***mycarenet@intermut.be***

3.5.3 Technical contact center MyCareNet:

Telephone: 02/431 47 71

Mail: ***ServiceDesk@MyCareNet.be***

4 Global overview



The eAttest WS is secured with the SAML HOK policy. Therefore, prior to calling the services, a SAML token must be obtained at the eHealth STS. The obtained token must be then included in the header of the request message, where the timestamp and the body must be signed with the certificate as used in the HOK profile of the SAML token (more detailed technical description can be found further in the chapter 5 of this cookbook). The body contains the eAttest request. The eHealth ESB verifies the security (authentication, authorization, etc.) and forwards the request to MyCareNet. Then, the service returns the response delivered by the MyCareNet backend.

5 Step-by-step

5.1 Technical requirements

In order to test the service, the eHealth development team first has to create a test case. The rules to access the eAttest are the same in acceptation and in production.

Access rules:

- authentication with a care providers certificate;
- authentication with the certificate of a mandate holder.

The eHealth development team has to configure all test cases.

So, before doing any test, request your test cases from the eHealth development team (***info@ehealth.fgov.be***).

In order to implement a WS 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 (WS stack for the client implementation) can be used instead.

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

Alternatively, you can write your own implementation. The usage of the STS and the structure of the exchanged xml-messages are described in the eHealth STS cookbook.

- ***https://www.ehealth.fgov.be/ehealthplatform/fr/service-iam-identity-access-management***
- ***https://www.ehealth.fgov.be/ehealthplatform/nl/service-iam-identity-access-management***

5.1.1 Use of the eHealth SSO solution

This section specifies how to call the STS in order to have access to the WS. You must precise several attributes in the request. The details on the identification attributes and the certification attributes can be found in the separate document eAttest_SSO.

To access the eAttest WS, the response token must contain “true” for all of the ‘boolean’ certification attributes and a non-empty value for other certification attributes.

If you obtain “false” or empty values, contact the eHealth platform to verify that they correctly configured the requested test case.

5.1.2 Encryption

All the information about the use of the encryption libraries and the call to the eHealth Token Key (ETK) 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. By example, 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

5.1.3 Security policies to apply

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

To call the eAttest WS:

- Add the business message to the soap body
- 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 (HOK)).
  - **Timestamp**
  - A **signature** that has been placed on the SOAPBody and the timestamp 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 and the Timestamp.
  - KeyInfo with a SecurityTokenReference pointing to the SAML Assertion.

See also the WSSP in the WSDL[4] (also included in the documentation).

5.2 Web service

The eAttest WS has one operation available:

- SendAttestation

The eAttest WS has the following endpoints:

- Pilot environment: ***https://services-acpt.ehealth.fgov.be/MyCareNet/eAttest/v1***
- Production environment: ***https://services.ehealth.fgov.be/MyCareNet/eAttest/v1***

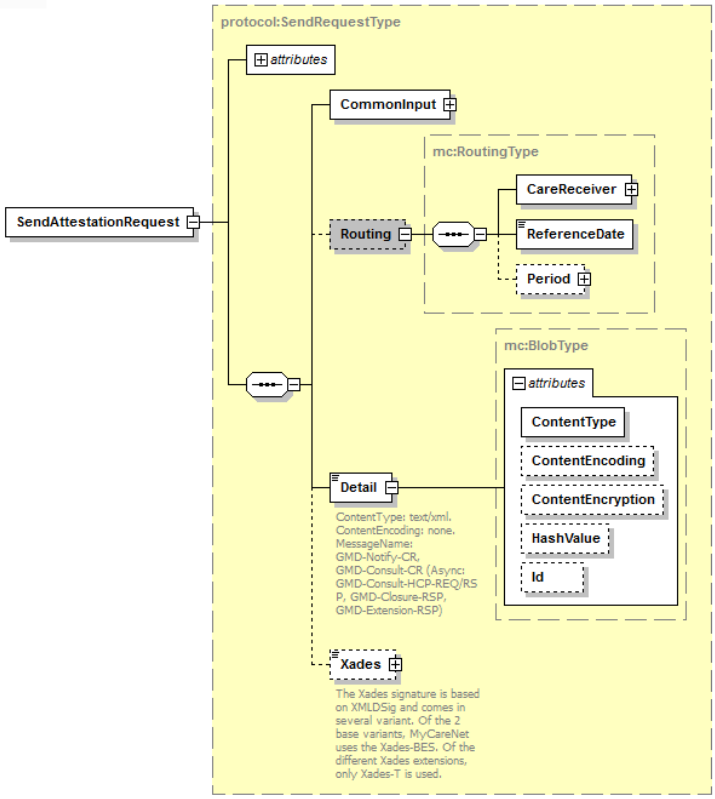
The remainder of this section describes the structure of the request and the response messages. Section 5.2.1 describes the request and response messages for the SendAttestation operation, and section 5.2.2 describes the common element types used in the structures of the request and response types. For more details on the specific elements and the concepts behind them, see the documentation as provided by the CIN/NIC on their Sharepoint.

5.2.1 Method SendAttestation

The goal of this method is to send the healthcare provided certificate to the insurance institutions. The response returned is an acknowledgement with a summary of the forwarded information.

[4] WSDL's can be found in the eHealth Service Registry: https://services.ehealth.fgov.be/registry/uddi/bsc/web

5.2.1.1 Input arguments in SendAttestationRequest



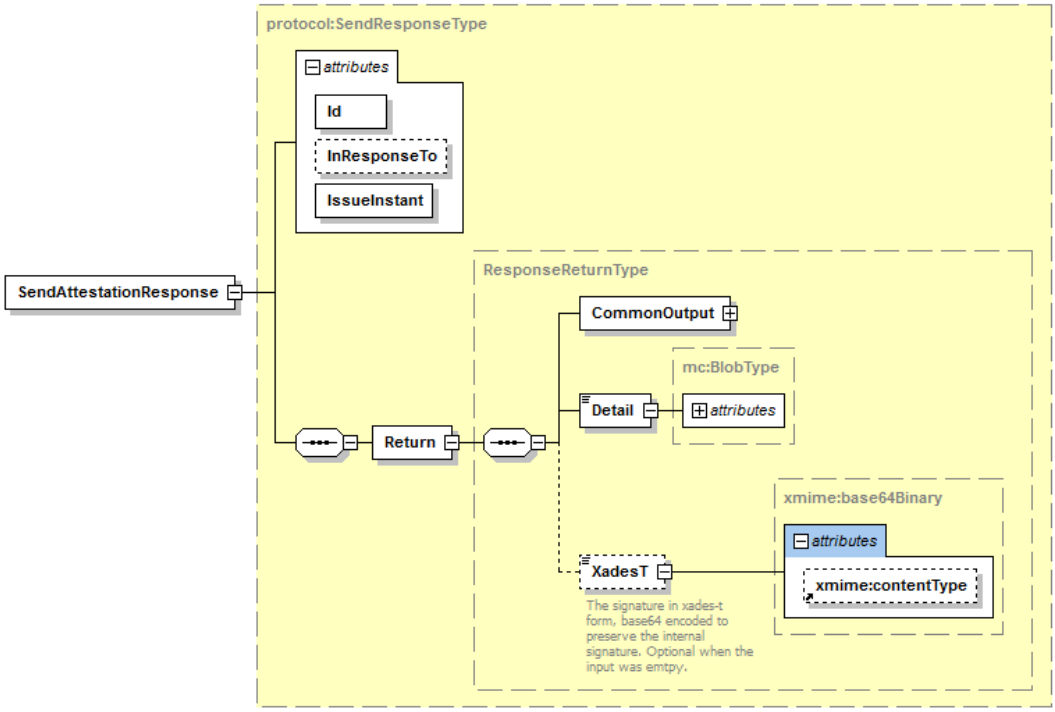
Field name	Description
CommonInput	See section 5.2.2.1 : CommonInputType
Routing	Mandatory element. See the documentation 'Service_Catalogue_Commons' provided by the CIN/NIC. The data within this element should contain either the SSIN of the care receiver either the combination *health insurance organization/identification number of the care receiver within this organization*

Detail	Encrypted detail of the request. The content of the encrypted message should respect some standard format to allow additional information exchange: - The identity of the Key to be used to encrypt the response. - The XAdES as probative force of the message. See the documentation provided by the CIN/NIC for more details about the structure "EncryptedKnownContent": - 'Service_Catalogue_GenSync' Attribute values : @ContentType: "text/xml" @ContentEncoding: "none" *@ContentEncryption*: attribute used to indicate if the content of the blob has been encrypted. The value should be - "encryptedForKnownCINNIC": the sender encrypted the content of the body with the public key of the CINNIC. @HashValue pre-calculated hash of the uncompressed and decoded content. Is always provided to the care provider. @Id: The ID of the blob for usage in the XAdES signature. It is an "NCName" instead of an "ID" in order to be able to have different blobs with the same (fixed) id without causing an XSD validation. Note that the attribute "MessageName" in the Detail element is not present in the interface as provided by eHealth. This attribute value is then filled out by the eHealth platform according to the called operation (for the eAttest service it is "E-ATTEST").
Xades	For eAttest, the Xades must be inserted in the "EncryptedKnownContent" structure. See the documentation provided by the CIN/NIC for more details about the structure "EncryptedKnownContent": - 'Service_Catalogue_GenSync'

5.2.1.2 Request example

Business example is generated from the documentation 'Kmehr - eAttest - V02R00.pdf' provided by CIN/NIC.

5.2.1.3 Output arguments in SendAttestationResponse



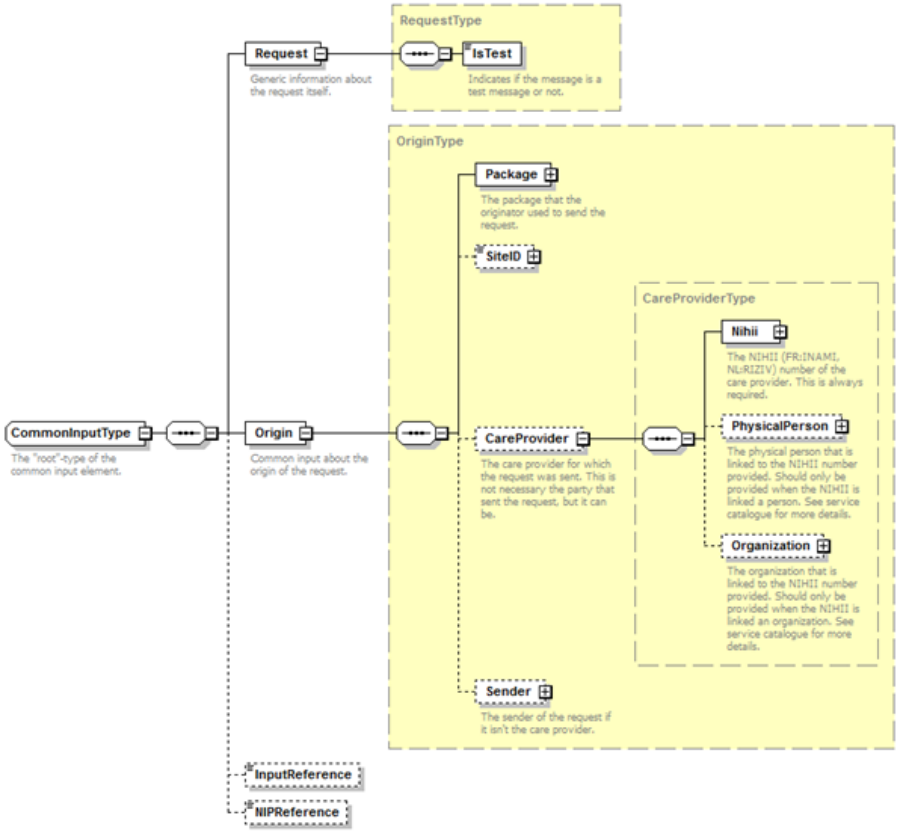
Field name	Description
"Response"	@Id: Unique Id for tracing @InresponseTo: 'Id' attribute of the request if available @IssueInstant: Generation response moment
Return	See the documentation provided by the CIN/NIC for more details : - 'Service_Catalogue_GenSync' - 'Kmehr - eAttest - V02R00.pdf' NB: In this case, the attribute *@ContentEncryption* can only have the value "encryptedForKnownHCP" (the content of the body is encrypted with the public key of the health-care provider).

5.2.1.4 Response example

Business example is generated from the documentation 'Kmehr - eAttest - V02R00.pdf' provided by CIN/NIC.

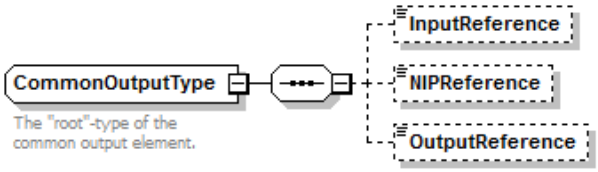
5.2.2 Used Types

5.2.2.1 CommonInputType



For the semantics of the particular elements and other information about the service, see the documentation Service_Catalogue_Commons and MyCareNet Authentication Catalogue provided by the CIN/NIC.

5.2.2.2 CommonOutputType



For the semantics of the particular elements and other information about the service see the documentation Service_Catalogue_Commons provided by the CIN/NIC

6 Security

6.1 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 (see Chap 3).

In case the eHealth platform finds a bug or vulnerability in its software, we advise the partner 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 us immediately. He is not allowed to publish this bug or vulnerability in any case.

6.2 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. Note that the time-to-live is the time difference between the Created and Expires elements in the Timestamp and is not related to the timeout setting on the eHealth ESB, etc. This means that eHealth will process the message if it is received within the time-to-live value (there is also tolerance of 5 minutes to account for the clock skew), but the actual response time may be greater than one minute in some situations.
- Signature of the timestamp and body. This will allow eHealth to verify the integrity of the message and the identity of the message author.
- Encryption of the business part of the message with the MyCareNet ETK.

7 Test and release procedure

7.1 Procedure

This chapter explains the procedures for testing and releasing an application in acceptation or production.

7.1.1 Initiation

If you intend to use the eHealth service in the acceptance environment, please contact ***info@ehealth.fgov.be***. The Project department will provide you with the necessary information and mandatory documents.

7.1.2 Development and test procedure

You have to develop a client in order to connect to our web service. Most of the required integration info to integrate is published in the technical library on the eHealth portal.

In some cases, the eHealth platform provides you with a mock-up service or test cases in order for you to test your client before releasing it in the acceptance environment.

7.1.3 Release procedure

When development tests are successful, you can request to access the eHealth acceptance environment.

From this moment, you can start integration and acceptance tests. The eHealth platform suggests testing during minimum one month.

After successful acceptance tests, the partner sends his test results and performance results with a sample of "eHealth request" and "eHealth answer" to the eHealth point of contact by email.

Then the eHealth platform and the partner agree on a release date. The eHealth platform prepares the connection to the production environment and provides the partner with the necessary information. During the release day, the partner provides the eHealth platform with feedback on the test and performance tests.

For further information and instructions, please contact: ***integration-support@ehealth.fgov.be***.

7.1.4 Operational follow-up

Once in production, the partner using the eHealth service for one of his applications will always test first in the acceptance environment before releasing any adaptations of his application in production. In addition, he will inform eHealth on the progress and test period.

7.2 Test cases

eHealth recommends performing tests for the following case:

- SendAttestation (contact NIC/CIN for test data of the patients)

In addition, the organization should also run negative test cases.

8 Error and failure messages

There are different possible types of response:

- If there are no technical errors, responses as described in section 5 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. For possible business errors, refer to the documentation 'GenericSync Error codes' and 'Service_Catalogue_Commons' provided by the CIN/NIC.

Table 1: Description of the possible SOAP fault exceptions.

Error code	Component	Description	Solution/Explanation
SOA-00001		Service error	This is the default error sent to the consumer in case more details are unknown.
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 the default error for content related errors in case more details are unknown.
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.

If the cause is a business error, please contact MyCareNet at 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 so when available, please provide it when requesting support.