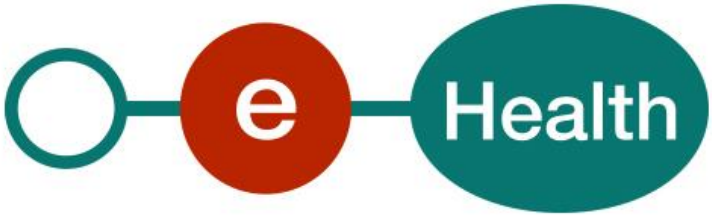


Global Medical File WS
Cookbook
Version 1.7

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

eHealth platform

Willebroekkaai 38 – 1000 Brussel

38, Quai de Willebroek – 1000 Bruxelles

Anyone is free to distribute this document, referring to the URL source.

Table of contents

Contents

Table of contents **2**

1. Document management **4**

1.1 Document history 4

2. Introduction **5**

2.1 Goal of the service 5

2.2 Goal of the document 5

2.3 eHealth platform document references 5

2.4 External document references 6

3. Support **7**

3.1 Helpdesk eHealth platform 7

3.1.1 Certificates 7

3.1.2 For issues in production 7

3.1.3 For issues in acceptance 7

3.1.4 For business issues 7

3.2 Status 7

3.3 Support desk – contact points CIN/NIC 7

3.3.1 Business support 7

3.3.2 MyCareNet Helpdesk: 7

3.3.3 Technical contact centre MyCareNet: 8

4. Global overview **9**

5. Step-by-step **10**

5.1 Technical requirements 10

5.1.1 Use of the eHealth SSO solution 10

5.1.2 Encryption 10

5.1.3 Security policies to apply 10

5.1.4 WS-I Basic Profile 1.1 11

5.1.5 Tracing 11

5.2 Web service 11

5.2.1 Method consultGlobalMedicalFile 12

5.2.2 Method notifyGlobalMedicalFile 14

5.2.3 Used types 17

6. Risks and security **18**

6.1 Security 18

6.1.1 Business security 18

6.1.2 Web service 18

6.1.3 The use of username, password and token 18

7. Test and release procedure **19**

7.1 Procedure 19

7.1.1 Initiation 19
7.1.2 Development and test procedure 19
7.1.3 Release procedure 19
7.1.4 Operational follow-up 19
7.2 Test cases 19
8. Error and failure messages 20

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	20/12/2012	eHealth platform	First version
1.1	12/11/2013	eHealth platform	Business error handling
1.2	24/03/2014	eHealth platform	Add Sharepoint CIN document references
1.3	20/04/2016	eHealth platform	Add SSO solution for dentist
1.4	15/02/2017	eHealth platform	Precisions par. 3.2
1.5	04/09/2018	eHealth platform	Update
1.6	15/05/2020	eHealth platform	WS-I Compliance
1.7	28/07/2022	eHealth platform	§ 3.2 Status (added) § 3.3 Support desk – contact points CIN/NIC (updated) § 5.1.5 Tracing (added)

2. Introduction

2.1 Goal of the service

Global Medical File (GMF) web services (WS) allow a physician to access a patient's administrative data and the transfer of the GMF to another healthcare provider (this service is not accessible by a specialist).

The healthcare professionals need to request a SAML token from eHealth Secure-Token-Service (STS) prior to calling the GMF services.

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 platform service.

However, in order to interact in a smooth, homogeneous and risk controlled way with a maximum of partners, eHealth platform 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 platform service in the client application.

Detailed description of the functionality of the services, the semantics of the particular elements and other general information about the services is out of the scope of this document. This kind of information can be found in the documentation provided by MyCareNet (CIN/NIC) on their share point.

In order to be able to test the GMF application, you need to take the following steps (see Section 5):

1. Create a test case including an authorized healthcare professional: If the testing is done for a real healthcare actor, the real NIHII number of the healthcare actor can be used. Otherwise, you will receive a test NIHII number from the eHealth platform (you must indicate the professional category you want to test). You always need to request the configuration of the test cases at the eHealth platform.
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 GMF WS.

The process for production is also described in the second part of this cookbook.

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 ones, can be used for the eHealth platform service.

ID	Title	Version	Date	Author
1.	SOA – Error guide	1.0	10/06/2021	eHealth platform
2.	GMF SSO	1.1	04/09/2018	eHealth platform

[1] ***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, you should notify the eHealth service management[3], which will manage the maintenance of this document.

ID	Title	Source	Date	Author
1.	Basic Profile Version 1.1	http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html	24/08/2004	Web Services Interoperability Organization
2.	GMF-GenericSync Error codes (3).xls			GMF-GenericSync Error codes (3).xls
3.	ImplementationGuide_For_CareProvider.docx	N.A.	06/12/2012	NIC-CIN
4.	NIPPIN GenSync.zip			NIPPIN GenSync.zip
5.	Service_Catalogue_Commons.pdf			Service_Catalogue_Commons.pdf
6.	Service_Catalogue_GenSync (14)			Service_Catalogue_GenSync (14)
7.	CEB 20140123 - GMD Versie V01R02 NL.zip	N.A.	30/01/2014	NIC-CIN
8.	CEB 20140123 - Protocol en bijlage HCParty Versie V01R02 NL (1).zip	N.A.	30/01/2014	NIC-CIN
9.	CME 20140123 - DMG Version V01R02 FR			CME 20140123 - DMG Version V01R02 FR
10.	CME 20140123 - Protocole et Annexe HCParty Version V01R02 FR (1).zip			CME 20140123 - Protocole et Annexe HCParty Version V01R02 FR (1).zip
11.	MyCareNet Authentication Catalogue (19).pdf	N.A.	31/01/2014	NIC-CIN

[2] In order to have access to the Sharepoint, an account is needed. Use the following link to request it :

https://www.cin-nic.be/noussommes/contact OU ***https://www.nic-cin.be/contact***

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

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.

3.3 Support desk – contact points CIN/NIC

3.3.1 Business support

For business questions: MyCareNet Helpdesk (first line support)

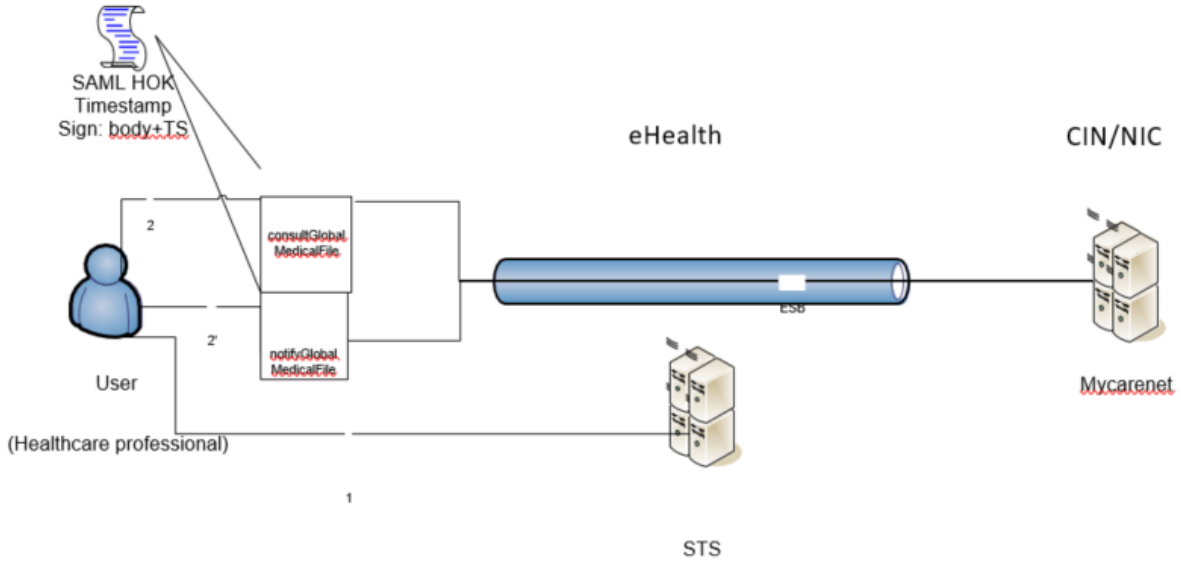
3.3.2 MyCareNet Helpdesk:

- Telephone: 02 891 72 56
- Mail: ***support@intermut.be***

3.3.3 Technical contact centre MyCareNet:

- Telephone: 02 431 47 71
- Mail: ***ServiceDesk@MyCareNet.be***

4. Global overview



The GMF services are secured with the SAML Holder-of-Key (HOK) policy. Therefore, prior to calling the services, a SAML token must be obtained at the eHealth STS (1). The obtained token must be then included in the header of the request message (2 or 2'), together with the timestamp, where the timestamp and the body must be signed with the certificate as used in the HOK profile of the SAML token (see also more detailed technical description further in the cookbook). The body contains the consultGlobalMedicalFile or notifyGlobalMedicalFile request (depending on the called service/operation). The eHealth ESB verifies the security (authentication, authorization, etc.) and forwards the request to MyCareNet.

5. Step-by-step

5.1 Technical requirements

In order to test the service (via STS), a test case must first be created by the eHealth platform. The rules to access the GMF WS are the same in acceptance environment as in production: authentication with a SAML token with a healthcare professional's certificate (see Section 3.1 for the information on the certificates and further in this section for the information about the SAML token).

Authentication with a SAML token (including the identity of the hospital and the healthcare professional) with a hospital's certificate. All test cases are to be configured by the eHealth platform.

Before doing any tests, request your test cases from the eHealth platform (info@ehealth.fgov.be).

The template "request testcases template" must be filled out completely. If you have any questions about the template, please contact 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 connector". Nevertheless, eHealth implementations use standards so 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.

5.1.1 Use of the eHealth SSO solution

This section specifies how to perform the call to STS in order to access the WS.

You must precise several attributes in the request. The separate document GMF SSO specifies the details on the identification attributes and the certification attributes.

To access the GenericInsurability 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 the requested test cases were correctly configured.

5.1.2 Encryption

Encryption (ETEE) is not used in the context of this project.

5.1.3 Security policies to apply

We expect that you use SSL one way for the transport layer. To call the GMF 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 will be added according the specifications of the OASIS SAML Token Profile (HOK).

    (http://www.oasis-open.org/committees/download.php/16768/wssv1.1-spec-os- SAMLTokenProfile.pdf).
  - 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 SOAP Body 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).

5.1.4 WS-I Basic Profile 1.1

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

5.1.5 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***

5.2 Web service

The GMF services have two separate WS: one for consulting the GMF of a patient and one for notifying the GMF of a patient. The GMF Consultation service has the operation *consultGlobalMedicalFile* and the GMF Notification service has the operation *notifyGlobalMedicalFile*.

The GMF Consultation WS has following endpoints:

- 6Integration environment: ***https://services-int.ehealth.fgov.be/GlobalMedicalFileConsultation/v1***
- Acceptance environment: ***https://services-acpt.ehealth.fgov.be/GlobalMedicalFileConsultation/v1***
- Production environment: ***https://services.ehealth.fgov.be/GlobalMedicalFileConsultation/v1***

The GMF Notification WS has following endpoints:

- Integration environment: ***https://services-int.ehealth.fgov.be/GlobalMedicalFileNotification/v1***
- Acceptance environment: ***https://services-acpt.ehealth.fgov.be/GlobalMedicalFileNotification/v1***
- Production environment: ***https://services.ehealth.fgov.be/GlobalMedicalFileNotification/v1***

The remainder of this section describes the structure of the request and the response messages.

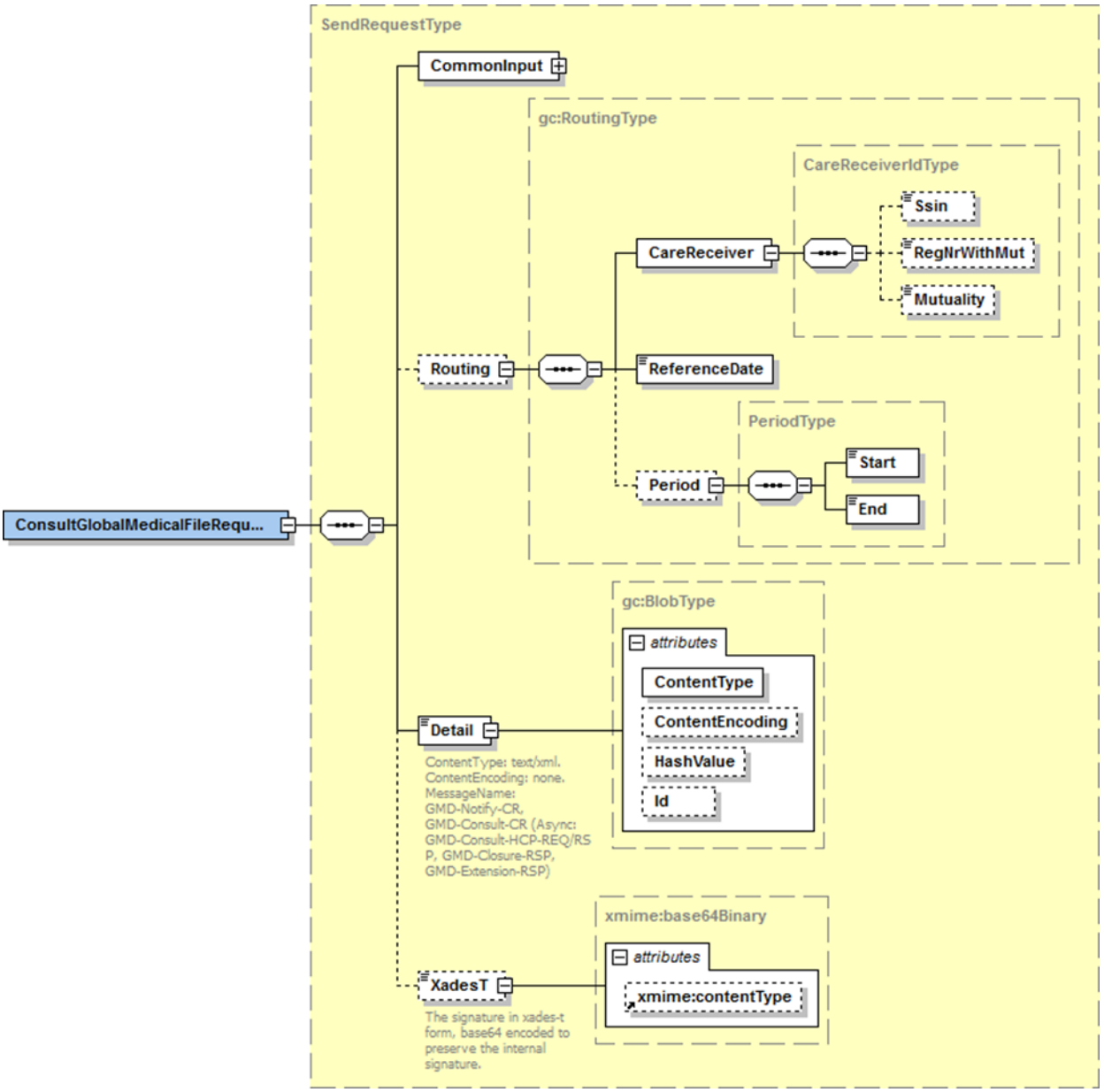
- Section 5.2.1 describes the request and response messages for the consultGlobalMedicalFile operation.
- Section 5.2.2 describes the request and response messages for the notifyGlobalMedicalFile operation.
- Section 5.2.3 describes the common element types used in the structures of the request and response 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.

[4] ***https://portal.api.ehealth.fgov.be/***

5.2.1 Method consultGlobalMedicalFile

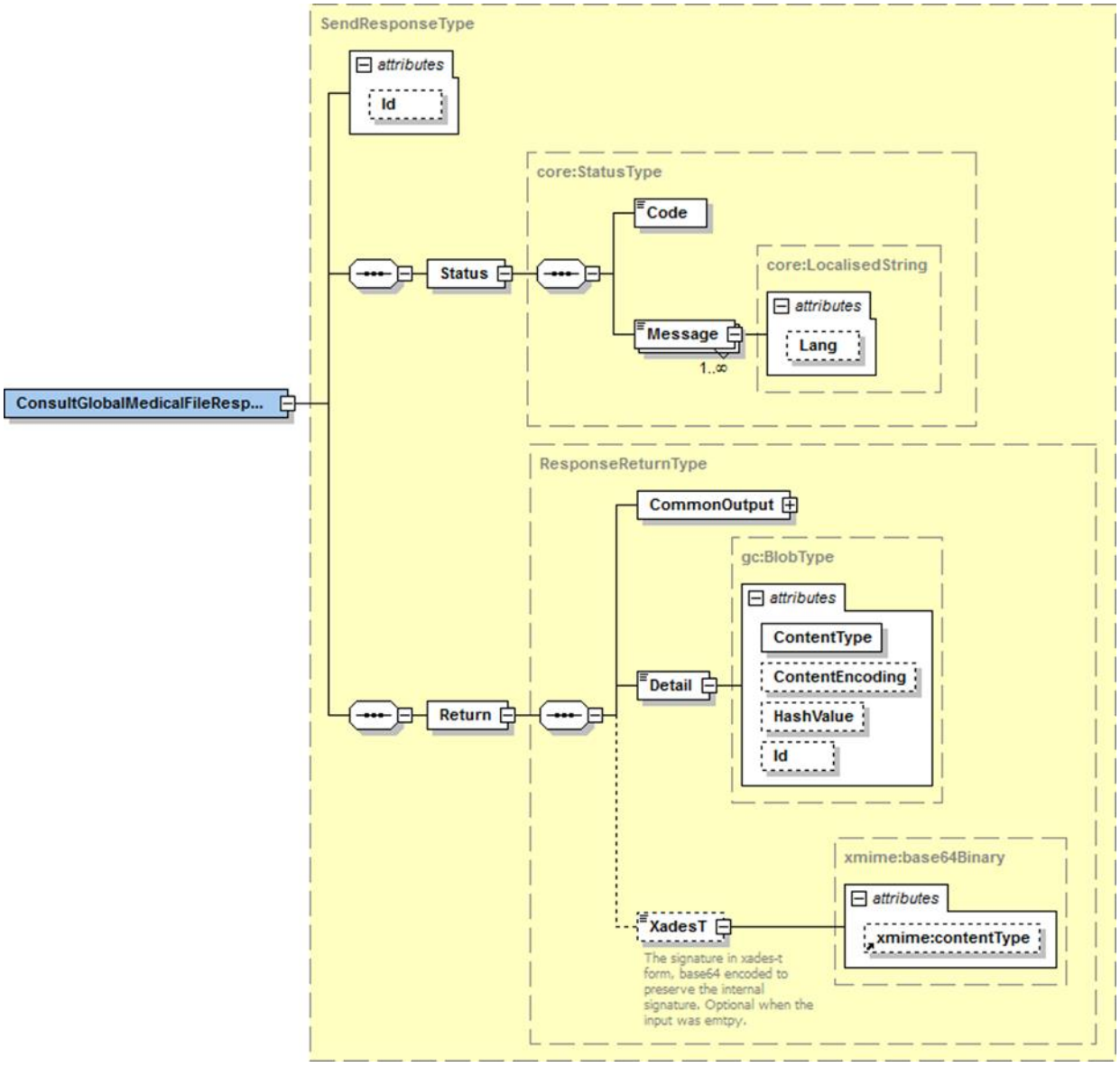
Input arguments in ConsultGlobalMedicalFileRequest



Field name	Description
CommonInput	See section 5.2.3.1
Routing	Mandatory element. See the documentation 'Service_Catalogue_Commons' provided by the CIN/NIC.
Detail	Base64 encoded detail of the request. See the documentation 'Service_Catalogue_GenSync (14)' and zip files provided by the CIN/NIC. Attribute values : @ContentType must be set to 'text/xml' @ContentEncoding must be set to'none' @HashValue 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 consultGlobalMedicalFile it is “GMD- Consult-CR”).
XadesT	Not mandatory

Output arguments in ConsultGlobalMedicalFileResonse



Field name	Description
Status	The status element contains a code and a message. If no error has occurred during the call, the code is set to "200" and the Message is "Success". Otherwise, a SOAP fault exception is returned (see also Section 8).

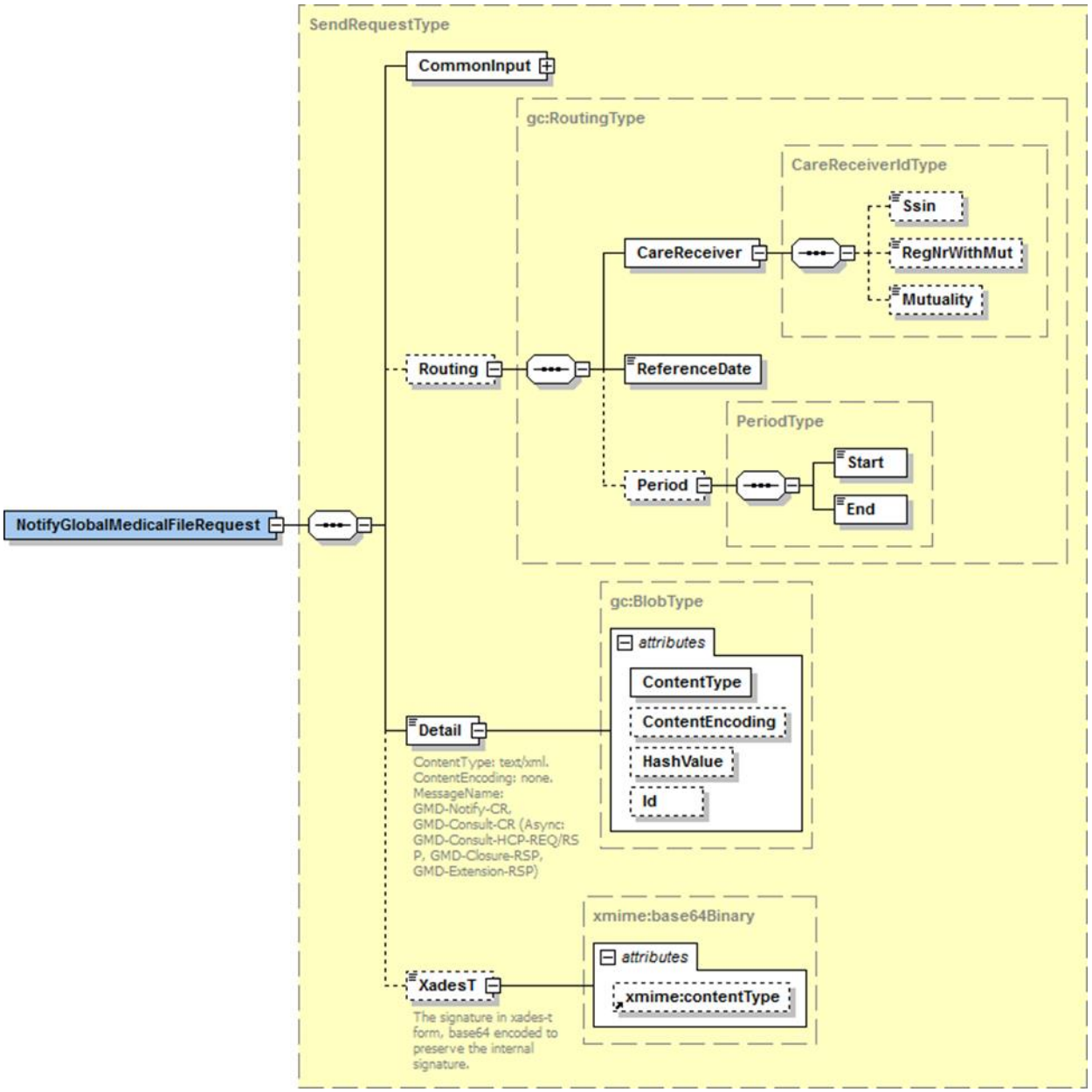
Return	See the documentation 'Service_Catalogue_GenSync (14)', 'Service_Catalogue_Commons' and zip files provided by the CIN/NIC.

Example

In the documentation provided by CIN/NIC, you can find business examples.

5.2.2 Method notifyGlobalMedicalFile

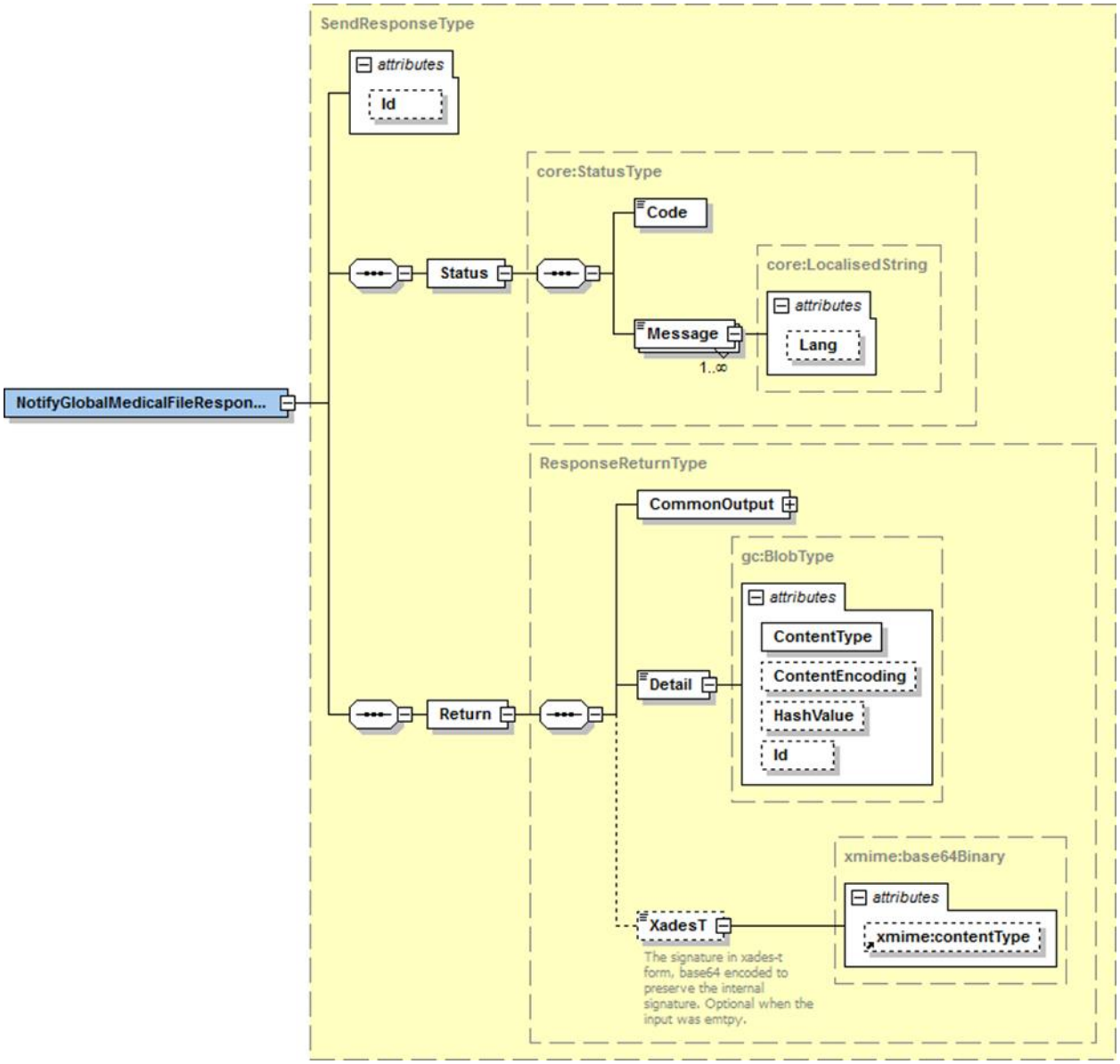
Input arguments in NotifyGlobalMedicalFileRequest



Field name	Description
CommonInput	See Section 5.2.3.1
Routing	Mandatory element. See the documentation 'Service_Catalogue_Commons' provided by the CIN/NIC
Detail	Base64 encoded detail of the request. See the documentation

	'Service_Catalogue_GenSync (14)' and zip files provided by the CIN/NIC. Attribute values : @ContentType must be set to 'text/xml' @ContentEncoding must be set to'none' @HashValue 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 the eHealth platform. This attribute value is then filled out by the eHealth platform according to the called operation (for the notifyGlobalMedicalFile it is "GMD-Notify-CR").
XadesT	A XAdES-BES is required (no timestamp). See the documentation 'Service_Catalogue_Commons' provided by the CIN/NIC.

Output arguments in NotifyGlobalMedicalFileResonse



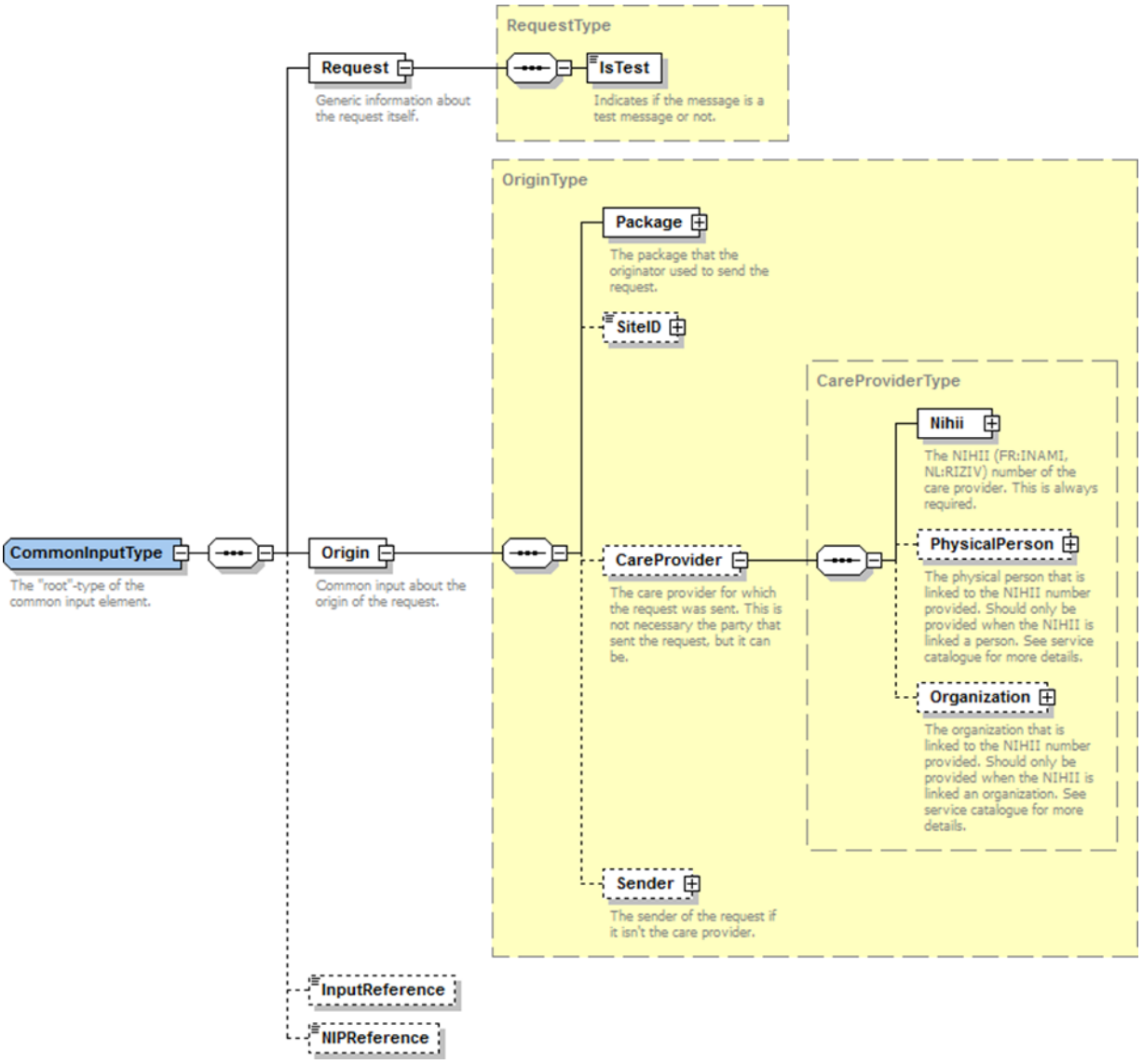
Field name	Description
Status	The status element contains a code and a message. If no error has occurred during the call, the Code is set to "200" and the message is "Success". Otherwise, a SOAP fault exception is returned (see also Section 8).
Return	See the documentation 'Service_Catalogue_GenSync (14)', 'Service_Catalogue_Commons' and zip files provided by the CIN/NIC.

Example

You can find business examples in the documentation provided by CIN/NIC.

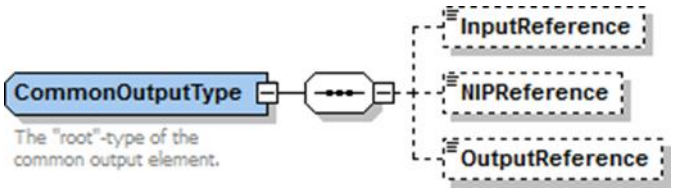
5.2.3 Used types

CommonInputType



For the semantics of the particular elements and other information about the service see the documentation Service_Catalogue_Commons and MyCareNet Authentication Catalogue (19) provided by the CIN/NIC.

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. Risks and security

6.1 Security

6.1.1 Business security

In case the development adds a use case based on an existing integration, the eHealth platform must be informed at least one month in advance. A detailed estimate of the expected load is necessary to be able to ensure an effective capacity management.

When technical issues occur on the WS, the partner can obtain support from the contact centre (see Chap 3)

If the eHealth platform should find a bug or vulnerability in its software, the partner must update his application with the latest version of the software, within ten (10) business days.

If the partner finds a bug or vulnerability in the software or web service made available by the eHealth platform, he is obliged to contact and inform us immediately. He is not allowed, under any circumstances, to publish this bug or vulnerability.

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. Note that the time-to-live is the time difference between the Created and Expired elements in the Timestamp and is not related to the timeout setting on the eHealth ESB, etc. This means that the eHealth platform 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 (see the SLA for more details).
- Signature of the timestamp and body. 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.

6.1.3 The use of username, password and token

The username, password, and token are strictly personal.
Every user takes care of his username, password and token, and he is forced to confidentiality of it. It is prohibited to transfer them to partners and clients. Until inactivation, every user is responsible for every use, including the use by a third party.

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 platform service, 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 WS. Most of the information needed to integrate is published on the portal of the eHealth platform.

Upon request and depending on the case, the eHealth platform provides you with a **test case** 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 acceptance environment of the eHealth platform. From this moment, you start the integration and acceptance tests. The eHealth platform suggests testing during minimum one month.

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

Once a release date has been agreed on, 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 platform service for one of his applications will always test in the acceptance environment first before releasing any adaptations of his application in production. In addition, he will inform the eHealth platform on the progress and test period.

7.2 Test cases

eHealth recommends performing tests for all of the following cases:

consultGlobalMedicalFile and notifyGlobalMedicalFile (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 documentation GMF-GenericSync Error codes (3) provided by 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 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 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

If the cause is a business error, please contact Mycarenet at *ServiceDesk@MyCareNet.be*.

Business error example :

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Server</faultcode>
      <faultstring>INCORRECT_INSS_DOCTOR_SAML</faultstring>
      <detail>
        <urn:BusinessError Id="urn:uuid:dcdc1fe0-6458-4e38-
b954-65fe4f6931dc"
xmlns:urn="urn:be:fgov:ehealth:errors:soa:v1">
          <Origin>MYCARENET</Origin>
          <Code>INCORRECT_INSS_DOCTOR_SAML</Code>
          <Message xml:lang="en">For 'doctor' the SSIN '12345678912' in the CareProvider element must
correspond to the 'urn:be:fgov:person:ssin' attribute in the saml '23456789123'</Message>
          <urn:Environment>Acceptation</urn:Environment>
        </urn:BusinessError>
      </detail>
    </soapenv:Fault>
</soap
env:Bo
  dy>
</soap
env:En
velope
  >
```

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.