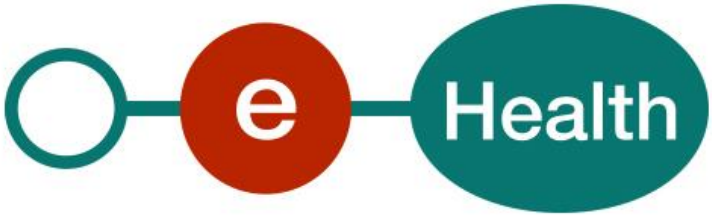


MyCareNet eAttest WS V3
Cookbook
Version 1.2

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

eHealth platform

Willebroekkaai 38 – 1000 Brussel

38, Quai de Willebroek – 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	22/07/2021	eHealth platform	First version
1.1	11/03/2022	eHealth platform	§3.2 Support MyCareNet
1.2	04/08/2022	eHealth platform	§ 5.1.5 Tracing (updated)

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 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, the latter must commit to comply with the requirements of specifications, data format, and release processes of the eHealth platform as described.

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	Date	Author
1	SOA – Error guide	1.0	10/06/2021	eHealth platform
2	***Request test case template***	3.0	22/02/2018	eHealth platform
3	MyCareNet eAttest V3 - SSO	1.0	22/07/2021	eHealth platform

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

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.

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	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	CIN Messages definition eattest v3	SharePoint Intermut	12/05/2021	CIN/NIC
3	E-AttestV3-Cancel-sample-request-new	SharePoint Intermut	14/07/2021	CIN/NIC
4	E-AttestV3-sample-request-new	SharePoint Intermut	09/07/2021	CIN/NIC
5	GenericSync Error codes	SharePoint Intermut	11/05/2021	CIN/NIC
6	ImplementationGuide_For_CareProvider	SharePoint Intermut	11/05/2021	CIN/NIC
7	MyCareNet Authentication Catalogue	SharePoint Intermut	11/05/2021	CIN/NIC
8	NIPPIN GenSync V4 (ESB 2 NIPPIN)	SharePoint Intermut	09/07/2021	CIN/NIC
9	Service_Catalogue_iSocial_Commons	SharePoint Intermut	09/07/2021	CIN/NIC
10	Service_Catalogue_iSocial_GenSync	SharePoint Intermut	12/05/2021	CIN/NIC
11	xsd-encryption	SharePoint Intermut	11/05/2021	CIN/NIC
12	BE-KERR-EAT3-ALL Codes erreurs eAttestV3 - Verwerpingscodes eAttestV3 - v03r01	SharePoint Intermut	08/06/2021	CIN/NIC

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

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

13	BE-KERR-EATN-ALL Codes erreurs eAttest Annulation - Verwerpingscodes eAttest Annulatie	SharePoint Intermut	16/03/2021	CIN/NIC
14	BE-LIST-EAT3-ALL liste des codes spécifiques - specifiek codes	SharePoint Intermut	17/03/2021	CIN/NIC
15	BE-MBSE-EAT3-ALL Matrix by sector - eAttestV3 v03r01	SharePoint Intermut	28/05/2021	CIN/NIC
16	BE-XLMS-EAT3-ALL examples v03	SharePoint Intermut	08/04/2021	CIN/NIC
17	cross check eAttest cancel	SharePoint Intermut	16/03/2021	CIN/NIC
18	cross check eAttest v3	SharePoint Intermut	16/03/2021	CIN/NIC
19	FR-FUNC-EAT3-ALL-Description fonctionnelle - eAttestV3 v03r01	SharePoint Intermut	11/05/2021	CIN/NIC
20	FR-FUNC-EATN-ALL Description fonctionnelle - eAttest Annulation v01r01	SharePoint Intermut	16/03/2021	CIN/NIC
21	FR-GLIN-EATN-ALL Guidelines eAttest Annulation	SharePoint Intermut	16/03/2021	CIN/NIC
22	FR-KHCP-MULT-ALL KMEHR - Annexe HCPARTY - V01r05	SharePoint Intermut	28/04/2021	CIN/NIC
23	FR-KLAY-EAT3-ALL Layout KMEHR - eAttestV3 v03r01	SharePoint Intermut	28/04/2021	CIN/NIC
24	FR-KLAY-EATN-ALL Layout KMEHR - Annulation eAttest v01r03	SharePoint Intermut	08/04/2021	CIN/NIC
25	FR-KPRO-MULT-ALL KMEHR - Protocole eHealth message service - V01r06	SharePoint Intermut	17/03/2021	CIN/NIC
26	NL-FUNC-EAT3-ALL-Functionele Beschrijving - eAttestV3 v03r01	SharePoint Intermut	11/05/2021	CIN/NIC

27	NL-FUNC-EATN-ALL Functionele beschrijving - eAttest Annulatie v01r01	SharePoint Intermut	16/03/2021	CIN/NIC
28	NL-GLIN-EATN-ALL Guidelines eAttest Annulatie	SharePoint Intermut	16/03/2021	CIN/NIC
29	NL-KHCP-MULT-ALL KMEHR - Bijlage HCPARTY - V01r05	SharePoint Intermut	28/04/2021	CIN/NIC
30	NL-KLAY-EAT3-ALL Layout KMEHR - eAttestV3 v03r01	SharePoint Intermut	28/04/2021	CIN/NIC
31	NL-KLAY-EATN-ALL Layout KMEHR - eAttest Annulatie v01r03	SharePoint Intermut	08/04/2021	CIN/NIC
32	NL-KPRO-MULT-ALL KMEHR - Protocol eHealth message service - V01r06	SharePoint Intermut	17/03/2021	CIN/NIC
33	xsd-kmehr message protocole-1_34	SharePoint Intermut	08/04/2021	CIN/NIC

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)

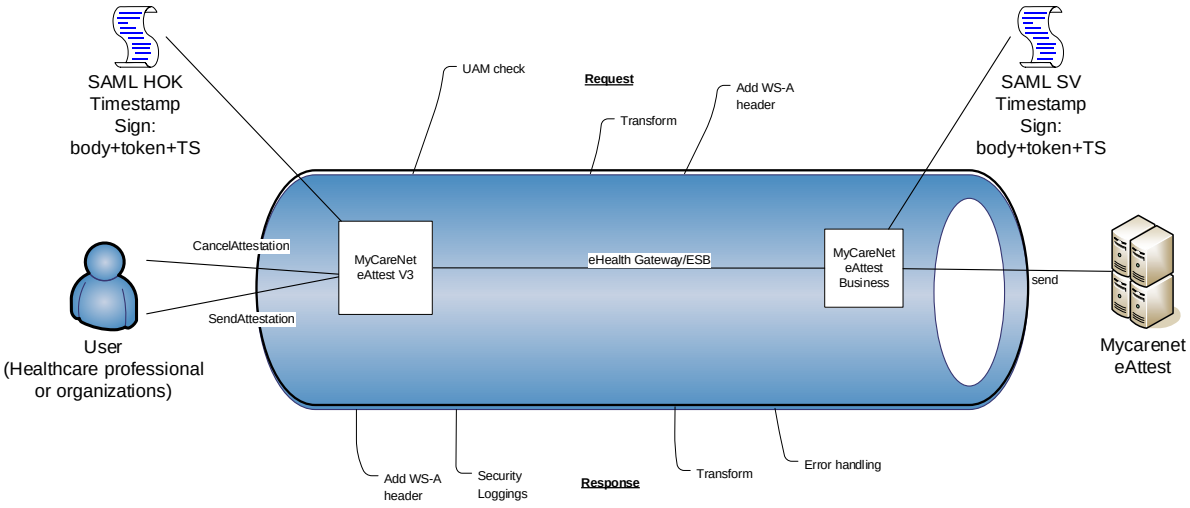
3.3.2 MyCareNet Helpdesk:

- 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 SAML Holder-of-Key (HOK) policy secures the eAttest service. Therefore, prior to calling the services, a SAML token must be obtained at the eHealth STS. The obtained token must then be included in the header of the request message. The timestamp and the body must be signed with the certificate as used in the HOK profile of the SAML token (See chapter 5). The body contains the eAttest request.

The eHealth Gateway/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 for acceptation and 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 but any other compatible technology (WS stack for the client implementation) can be used instead.

- ***https://www.ehealth.fgov.be/nl/support/connectors***
- ***https://www.ehealth.fgov.be/fr/support/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/nl/support/sts-secure-token-service***
- ***https://www.ehealth.fgov.be/fr/support/sts-secure-token-service***

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 specify several attributes in the request. The details on the identification attributes and the certification attributes can be found in the separate document MyCareNet eAttest V3 - SSO.

To access the eAttest WS, the response token must contain “true” for 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

In the End-To-End Encryption (ETEE) cookbooks on the portal of the eHealth platform, you will find all the information about the use of the encryption libraries and the call to the eHealth Token Key (ETK) deport.

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

Please note that only the SendAttestation method needs encryption.

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.

As web service 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: an eHealth certificate or a SAML token issued by STS.

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

The STS cookbook explains how to implement this security policy.

See: ***https://www.ehealth.fgov.be/ehealthplatform/STS-cookbook.pdf***

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 eAttest WS has two operations available:

- SendAttestation
- CancelAttestation

The eAttest WS has the following endpoints:

- Acceptation environment: ***https://services-acpt.ehealth.fgov.be/MyCareNet/eAttest/v3***
- Production environment: ***https://services.ehealth.fgov.be/MyCareNet/eAttest/v3***

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

- Section 5.5.1 describes the request and response messages for the SendAttestation operation;
- Section 5.5.2 describes the request and response messages for the CancelAttestation operation;
- Section 5.5.3 describes the common element types used in the structures of the request and response types.

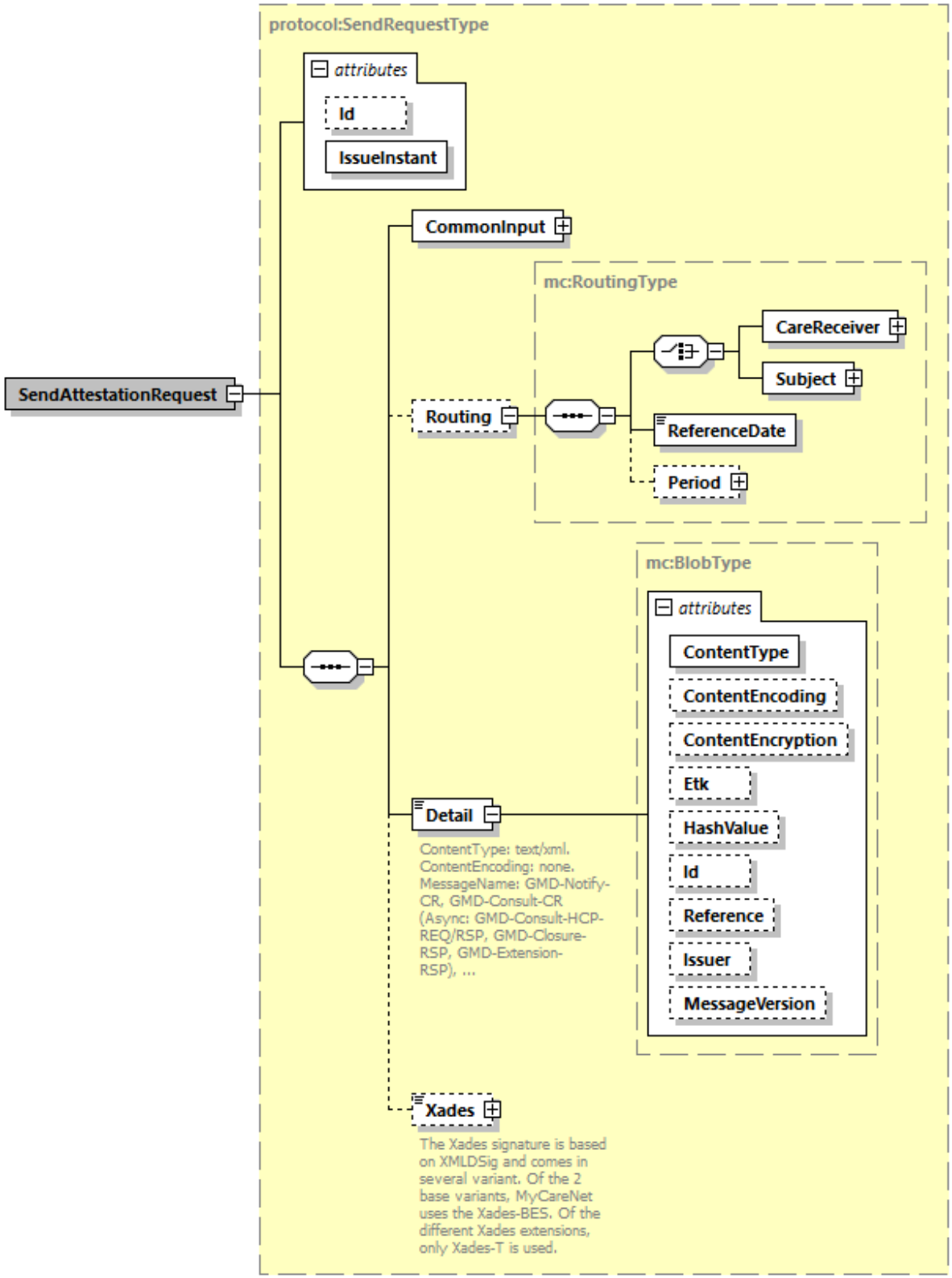
For more details on the specific elements and the concepts behind them, see the documentation as provided by the CIN/NIC on their Sharepoint.[4]

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] https://share.intermut.be/home/MyCareNet/Extranet

5.2.1.1 Input arguments in SendAttestationRequest



Field name	Description
CommonInput	See section 5.2.3.1 : CommonInputType

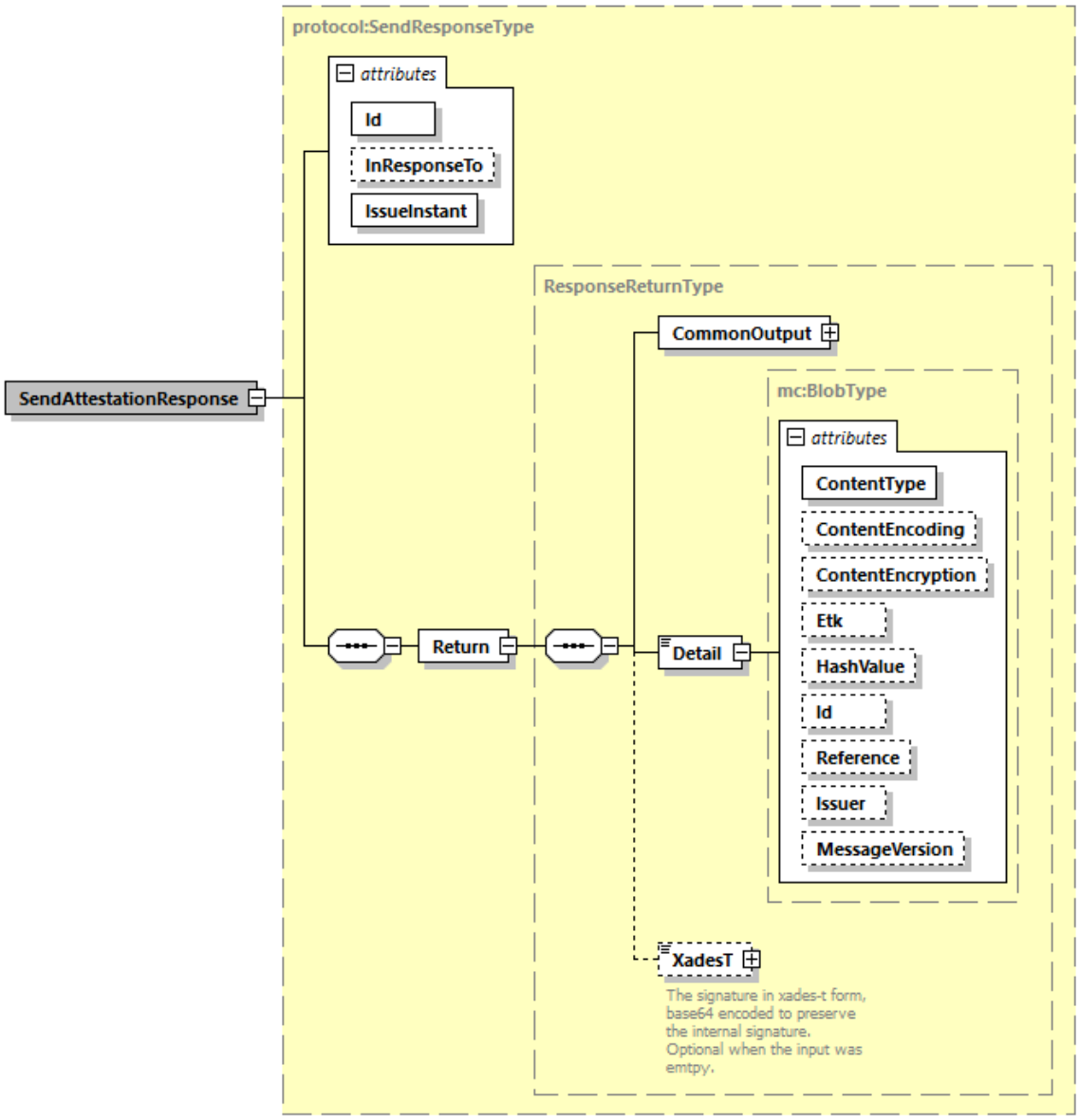
Routing	Optional element containing a choice : • CareReceiver : the data should contain either the SSIN of the care receiver, either the combination health insurance organization/identification number of the care receiver within this organization. • Subject : the data should represent a well-identified subject in the context of the request. Subject should not be used for eAttest v3. You should only use CareReceiver. See the documentation "Service_Catalogue_iSocial_Commons" provided by the CIN/NIC.
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_iSocial_GenSync". Attribute values : • ContentType : value must be "text/xml" • ContentEncoding : value must be "none" • ContentEncryption : value must be "encryptedForKnownBED" • ETK: the encryption token that has been used for the encryption of the body. Mentioning this information helps the recipient to identify the private key to be used for decryption. When not provided, the recipient may choose to reject the message or try to decrypt using the several existing private keys. • 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. • Reference : Reference of the exchanged blob. This may be used as correlation identifier with other messages (e.g. while confirming the reception of a message in genericAsync). Reference should not be used for eAttest v3. • Issuer : identification of the sender of the information. This information is provided only when relevant. • MessageVersion : version of the message used in the body. This can be used when different version of the message schema exists. The list of supported versions is documented with the definition of the message 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 in by the eHealth platform according to the called operation (for the SendAttestation message it is "E-ATTEST-V3").
XAdES	For the method SendAttestation of 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_iSocial_GenSync".

5.2.1.2 Request example

Business example can be retrieved in the documentation provided by the CIN/NIC :

- FR-KPRO-MULT-ALL KMEHR - Protocol eHealth message service - V01r06
- FR-KLAY-EAT3-ALL Layout KMEHR - eAttestV3 v03r01
- BE-XLMS-EAT3-ALL examples v03

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
CommonOutput	See section 5.2.3.2 : CommonOutputType

Detail	See the documentation provided by the CIN/NIC for more details : • "Service_Catalogue_iSocial_GenSync". • "FR-KPRO-MULT-ALL KMEHR - Protocol eHealth message service - V01r06" • "FR-KLAY-EAT3-ALL Layout KMEHR - eAttestV3 v03r01" NB: In this case, the attribute *@ContentEncryption* can only have the value "encryptedForKnownRecipient" (the content of the body is encrypted with the public key of the health-care provider).

5.2.1.4 Response example

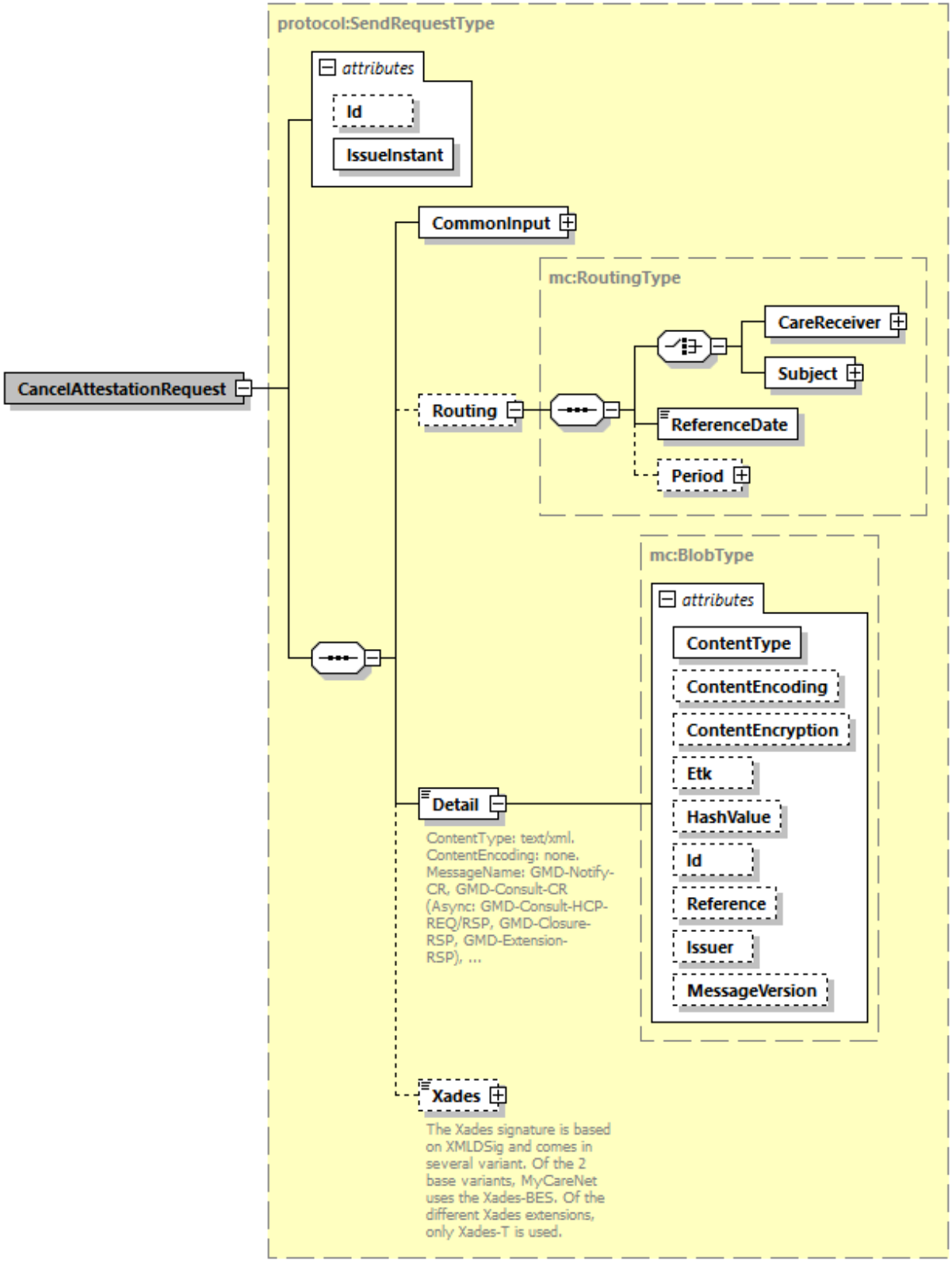
Business example can be retrieved in the documentation provided by the CIN/NIC :

- FR-KPRO-MULT-ALL KMEHR - Protocole eHealth message service - V01r06
- FR-KLAY-EAT3-ALL Layout KMEHR - eAttestV3 v03r01
- BE-XLMS-EAT3-ALL examples v03

5.2.2 Method CancelAttestation

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

5.2.2.1 Input arguments in CancelAttestationRequest



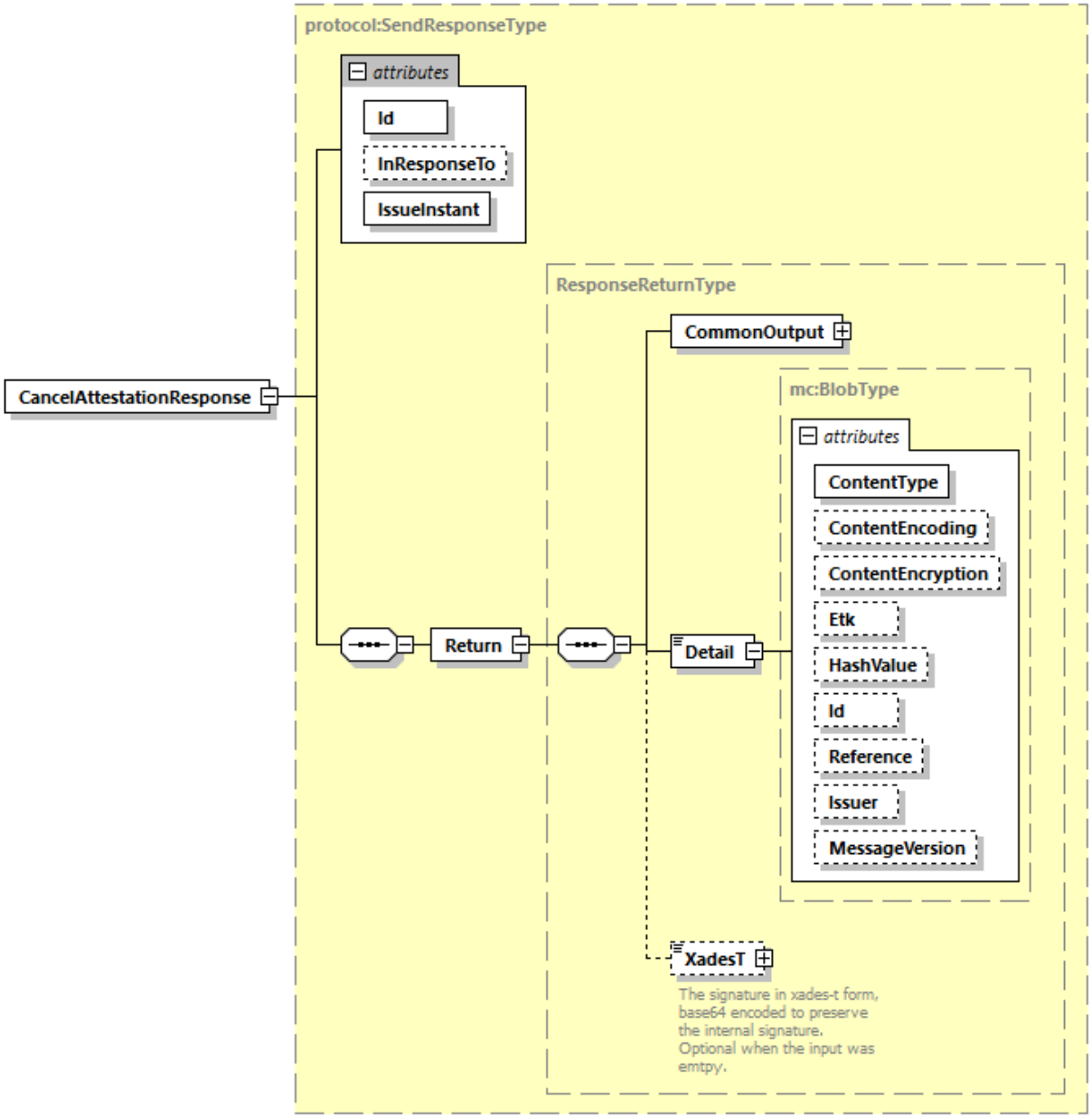
Field name	Description
CommonInput	See section 5.2.3.1 : CommonInputType
Routing	This element is not used and must not be specified for the CancelAttestation requests
Detail	Attribute values : • ContentType: “text/xml” • ContentEncoding: “none” • ContentEncryption: Must not be specified as the Cancel request is not encrypted • ETK: Must not be specified as the Cancel request is not encrypted • HashValue Must not be specified as the Cancel request is not encrypted • 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. • Reference : Reference of the exchanged blob. This may be used as correlation identifier with other messages (e.g. while confirming the reception of a message in genericAsync). Reference should not be used for eAttest v3. • Issuer : identification of the sender of the information. This information is provided only when relevant. • MessageVersion : version of the message used in the body. It can be used when different version of the message schema exists. The list of supported versions is documented with the definition of the message 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 in by the eHealth platform according to the called operation (for the CancelAttestation it is “E-ATTEST-CANCEL”).
XAdES	As this request is not encrypted, the XAdES must be put in this element Encoded in Base64

5.2.2.2 Request example

Business example can be retrieved in the documentation provided by the CIN/NIC :

- FR-KPRO-MULT-ALL KMEHR - Protocol eHealth message service - V01r06
- FR-KLAY-EATN-ALL Layout KMEHR - Annulation eAttest v01r03
- BE-XLMS-EAT3-ALL examples v03

5.2.2.3 Output arguments in CancelAttestationResponse



Field name	Description
"Response"	@Id: Unique Id for tracing @InresponseTo: 'Id' attribute of the request if available @IssueInstant: Generation response moment
CommonOutput	See section 5.2.3.2 : CommonOutputType
Detail	See the documentation provided by the CIN/NIC for more details : • 'Service_Catalogue_iSocial_GenSync' • 'FR-KPRO-MULT-ALL KMEHR - Protocol eHealth message service - V01r06' • 'FR-KLAY-EATN-ALL Layout KMEHR - Annulation eAttest v01r03'

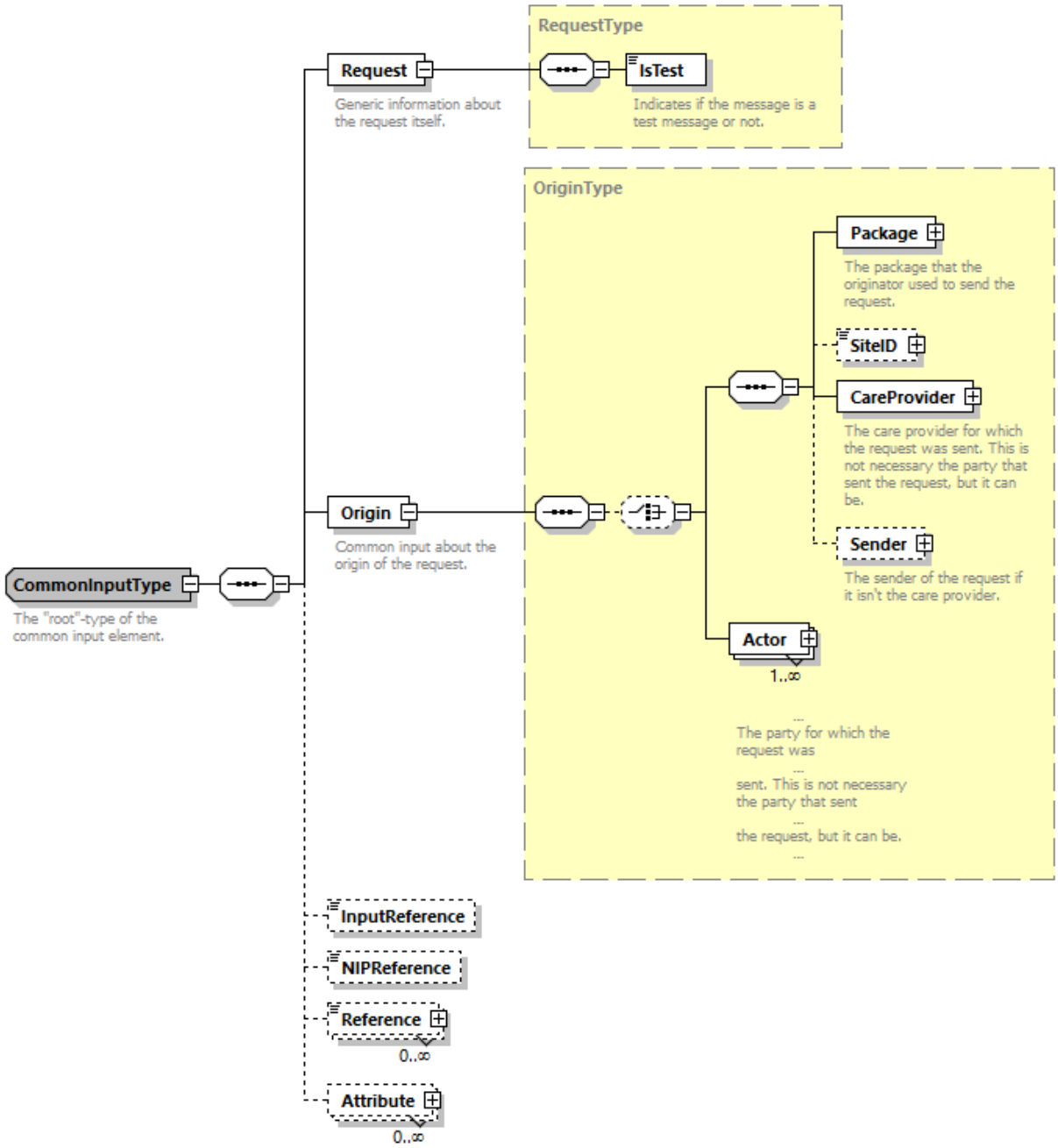
5.2.2.4 Response example

Business example can be retrieved in the documentation provided by the CIN/NIC :

- FR-KPRO-MULT-ALL KMEHR - Protocol eHealth message service - V01r06
- FR-KLAY-EATN-ALL Layout KMEHR - Annulation eAttest v01r03
- BE-XLMS-EAT3-ALL examples v03

5.2.3 Used Types

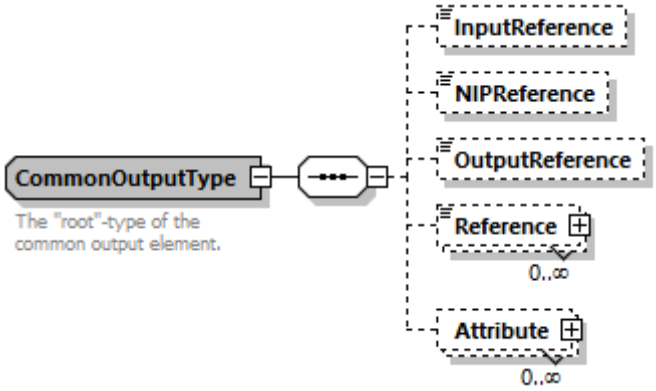
5.2.3.1 CommonInputType



Field name	Description
Request	Indicates the type of request, currently only debug or not.
Origin	Indicates where the message originates from. For the semantics of the particular elements and other information about the service see the documentation Service_Catalogue_iSocial_Commons provided by the CIN/NIC. Actor should not be used in eAttest v3.

InputReference	Reference filled in by the requester. This value can be returned in the corresponding response for correlation purposes. This reference is a feature of the message as a whole; a message may contain many records all sharing the same InputReference.
NipReference	NIPReference is a reference filled in by the iSocial platform.
Reference	Additional reference, typed, that can be used for different business cases. Reference should not be used in eAttest v3.
Attribute	Additional metadata on the request. Specific message description may also define business-specific metadata. Only standard attributes (urn:be:cin:nippin:purpose, urn:be:cin:nippin:attemptNbr) can be used in eAttest v3 (see the documentation Service_Catalogue_iSocial_Commons provided by the CIN/NIC)

5.2.3.2 CommonOutputType



Field name	Description
InputReference	Reference filled in by the requester. This value can be returned in the corresponding response for correlation purposes. This reference is a feature of the message as a whole; a message may contain many records all sharing the same InputReference.
OutputReference	Reference filled in by the requester. This value can be returned in the corresponding response for correlation purposes. This reference is a feature of the message as a whole; a message may contain many records all sharing the same OutputReference.
NipReference	NIPReference is a reference filled in by the iSocial platform.
Reference	Additional reference, typed, that can be used for different business cases. Reference should not be used in eAttest v3.
Attribute	Additional metadata on the request. Specific message description may also define business-specific metadata

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 center (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.
- Signature of the timestamp, body and binary security token. This allows the eHealth platform 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.

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 a minimum of 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

The eHealth platform recommends performing tests for all of the following cases:

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

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, you should receive the responses as described in section 5.
- In the case of a technical error, you will receive a SOAP fault exception as in the table below. For extensive explanation, please refer to "SOA – Error guide document" on the portal of the eHealth platform.

If an error occurs, first please verify your request.

The following table contains a list of common system error codes for the eHealth Service Bus/Gateway. For possible business errors, refer to the documentation "GenericSync Error codes" and "Service_Catalogue_iSocial_Commons" provided by the CIN/NIC.

Error code	Component	Description	Solution
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[5] in Registry/Repository.
SOA-03006	Consumer	XSD compliance failure	Message is not compliant with XSD in Registry/Repository.

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

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.