Service specification eHealth Chapter IV

Version 1.03

eHealth platform

Willebroekkaai 38,
38, Quai de Willebroeck

1000 BRUSSELS

Table of contents

1 Introduction

This document describes how send a request to the Chapter IV services. More in particular, it describes the security requirements and the structure of the messages (the interface of the service). 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 (CIN/NIC) (see the documentation contained in the "MyCareNet functional description 01.zip" archive).

In order to be able to call the Chapter IV web services, please follow these steps:

- Use the eHealth SSO authentication (see section 2).
- Use the eHealth Encryption libraries to encrypt the questionnaire before registration (see section 3).
- Call the web service:
    - Requests to the Chapter IV services are described in section 4.
    - Responses from the service are described in section 5.

The common elements used in requests and responses are described in section 6.

If you have technical questions or need more information, you can contact eHealth at info@ehealth.fgov.be.

2 Web service SSO Authentication - STS

This section specifies how to obtain a SAML token from the STS (Secure Token Service) in order to have access to the Chapter 4 Consult web service. There are different types of user, according to eHealth's Unique File, who are allowed to access Chapter 4 web services and act as author of operation's requests, therefore this document will be updated when the services are made available to a new type of user.

Each type of user needs a different type of token to access the services. The remainder of this section describes the needed attributes for each type of the user. For more details on how STS works, see

https://www.ehealth.fgov.be/fr/support/sts-secure-token-service (French version)

https://www.ehealth.fgov.be/nl/support/sts-secure-token-service (Dutch version)

2.1 The use of SAML holder-of-key solution

2.1.1 Physician

The request for the SAML token is secured with the eID[1] of the doctor. The certificate used by the Holder-Of-Key verification mechanism is an eHealth certificate[2].

The needed attributes are the following (AttributeNamespace: "urn:be:fgov:identification-namespace"):

- The social security identification number of the physician:
  - ***urn:be:fgov:person:ssin***
  - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin***

Physician must also specify which information must be asserted by eHealth:

- The social security identifier number of the doctor (AttributeNamespace: "urn:be:fgov:identification-namespace"):
  - ***urn:be:fgov:person:ssin***
  - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin***
- The physician uses his/her personal certificate (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth")
  - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin:usersession:boolean***
- To have access to the Chapter 4 Consult web service, the person must be a physician having valid visa and NIHII number (AttributeNamespace: urn:be:fgov:certifiednamespace:ehealth):
  - ***urn:be:fgov:person:ssin:ehealth:1.0:doctor:nihii11***

[1] *As fallback, in absence of the eID, the personal eHealth certificate can be used for authentication instead.*

[2] *The information about the eHealth certificates and the certificate requesting procedures can be found in the support section at https://www.ehealth.fgov.be/fr/support/presentation-du-support (French version) or https://www.ehealth.fgov.be/nl/support/presentatie-van-de-support (Dutch version)*

2.1.2 Pharmacy

Warning *!! Access is allowed to Chapter IV consultation only !!*

Pharmacies must specify several attributes in the request. The request to the STS is secured with the eID of the pharmacist starting the session. The certificate of the pharmacy issued by eHealth is used by the HOK mechanism. Pharmacies do not have access to the Chapter 4 Admission service.

The attributes that need to be provided in the request are the following (AttributeNamespace: urn:be:fgov:identification-namespace):

- The social security identifier number of the person starting the session (the person must be a recognized pharmacist):
  - ***urn:be:fgov:person:ssin***
  - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin***
- The identifier of the pharmacy:
  - ***urn:be:fgov:ehealth:1.0:pharmacy:nihii-number***
- The identifier of the pharmacy holder:
  - ***urn:be:fgov:person:ssin:ehealth:1.0:pharmacy-holder***

Pharmacies must also specify which information must be asserted by eHealth :

- The SSIN of the person (must be a pharmacist) starting the session, this is verified by eHealth (AttributeNamespace: urn:be:fgov:identification-namespace):
  - ***urn:be:fgov:person:ssin***
  - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin***
- The NIHII number of the pharmacy. The link between the pharmacy and the pharmacist starting the session is not verified, any pharmacist can start the session (AttributeNamespace: urn:be:fgov:identification-namespace):
  - ***urn:be:fgov:ehealth:1.0:pharmacy:nihii-number***
- The identifier of the pharmacy holder (SSIN), i.e. the pharmacist responsible for all activities performed in the pharmacy (AttributeNamespace: urn:be:fgov:identification-namespace):
  - ***urn:be:fgov:person:ssin:ehealth:1.0:pharmacy-holder***
- The identifier of the pharmacy holder (NIHII11), i.e. the pharmacist responsible for all activities performed in the pharmacy (AttributeNamespace: urn:be:fgov:certified-namespace:ehealth):
  - ***urn:be:fgov:person:ssin:ehealth:1.0:pharmacy-holder:certified:nihii11***
- The pharmacy must be a recognised pharmacy (AttributeNamespace: urn:be:fgov:certified-namespace:ehealth):
  - ***urn:be:fgov:ehealth:1.0:pharmacy:nihii-number:recognisedpharmacy:boolean***
- The pharmacy holder must be the certified pharmacy holder of the given pharmacy (AttributeNamespace: urn:be:fgov:certified-namespace:ehealth):
  - ***urn:be:fgov:ehealth:1.0:pharmacy:nihii-number:person:ssin:ehealth:1.0:pharmacy-holder:boolean***
- The person must be a recognized pharmacist (AttributeNamespace: urn:be:fgov:certifiednamespace:ehealth):
  - ***urn:be:fgov:person:ssin:ehealth:1.0:fpsph:pharmacist:boolean***

- The pharmacist uses his/her personal certificate (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth")
    - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin:usersession:Boolean***

2.1.3 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 (Attribute namespace: "urn:be:fgov:identification-namespace"):

- The NIHII number of the hospital:
    - ***urn:be:fgov:ehealth:1.0:hospital:nihii-number***
    - ***urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number***

Hospital must also specify which information must be asserted by eHealth:

- The NIHII number of the hospital (Attribute namespace: urn:be:fgov:identification-namespace):
    - ***urn:be:fgov:ehealth:1.0:hospital:nihii-number***
    - ***urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number***
- The hospital must be a recognized hospital (AttributeNamespace: urn:be:fgov:certified-namespace:ehealth):
    - ***urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number:recognisedhospital:boolean***

2.2 The use of SAML sender-vouches solution

2.2.1 Web Application CIVARS

WA Civars could be used either within a hospital or outside a hospital by a physician who is the only authorized user.

Outside a hospital

The needed attributes are the following (AttributeNamespace: "urn:be:fgov:identification-namespace"):

- The social security identification number of the physician:
    - ***urn:be:fgov:person:ssin***
    - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin***

Civars must also specify which information must be asserted by eHealth:

- The social security identifier number of the doctor (AttributeNamespace: "urn:be:fgov:identification-namespace"):
    - ***urn:be:fgov:person:ssin***
    - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin***
- The physician uses his/her personal certificate (AttributeNamespace: "urn:be:fgov:certified-namespace:ehealth")
    - ***urn:be:fgov:ehealth:1.0:certificateholder:person:ssin:usersession:boolean***
- To have access to Chapter 4, the person must be a physician having valid visa and NIHII number (AttributeNamespace: urn:be:fgov:certifiednamespace:ehealth):
    - ***urn:be:fgov:person:ssin:ehealth:1.0:doctor:nihii11***

Within a hospital

The needed attributes are the following (AttributeNamespace: "urn:be:fgov:identification-namespace"):

- The NIHII number of the hospital:
    - ***urn:be:fgov:ehealth:1.0:hospital:nihii-number***
    - ***urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number***

Civars must also specify which information must be asserted by eHealth:

- The NIHII number as identifier of the hospital (Attribute namespace: urn:be:fgov:identification-namespace):
    - ***urn:be:fgov:ehealth:1.0:hospital:nihii-number***
    - ***urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number***
- To have access to the Chapter 4, the hospital must be a recognized hospital (AttributeNamespace: urn:be:fgov:certified-namespace:ehealth):
    - ***urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number:recognisedhospital:boolean***

3 Encrypted message

All the information about the use of the encryption libraries and the call to the ETK (eHealth Token Key) depot are described in the End-To-End Encryption (ETEE) cookbooks
https://www.ehealth.fgov.be/fr/support/services-de-base/systeme-de-cryptage-end-to-end (FR)
https://www.ehealth.fgov.be/nl/support/basisdiensten/systeem-voor-end-end-vercijfering (NL)

To encrypt (addressed to CIN/NIC) the request parts, you have to call the GetEtk operation to pick up the right ETK from the eHealth ETK depot. The table below provides you the identifiers to use in the GetEtkRequest.

Environment	Type	Value	Application ID
Integration Test Environment	CBE	0820563481	MYCARENET
Acceptance Environment	CBE	0820563481	MYCARENET
Production Environment	CBE	0820563481	MYCARENET

The encryption to a HIO (unknown recipient encryption) is done with a symmetric key as obtained from the KGSS. In order to allow any HIO (but only a HIO) to decrypt the message, the key has to be requested with the allowed-reader specified with the following arguments:

- **Namespace:** urn:be:fgov:certified-namespace:ehealth
- **Name:** urn:be:fgov:kbo-bce:organization:cbe-number:ehealth:1.0:hio:boolean
- **Value:** true

For example:

```
<GetNewKeyRequestContent xmlns="urn:be:fgov:ehealth:etee:kgss:1_0:protocol">
    <AllowedReader>
        <Namespace>urn:be:fgov:certified-namespace:ehealth</Namespace>
        <Name>urn:be:fgov:kbo-bce:organization:cbe-number:ehealth:1.0:hio:boolean</Name>
        <Value>true</Value>
    </AllowedReader>
    <ETK>MIAGCS...</ETK>
</GetNewKeyRequestContent>
```

4 Request to the Chapter IV webservice

To call the Chapter IV webservice:

- 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 (holder-of-key). (link: 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 soapBody and the Timestamp.
    - KeyInfo with a SecurityTokenReference pointing to the SAML Assertion.

See also the WSSP in the WSDL[3].

As for now, only the operations described below are available (when support for new user types is added, additional operations will be added to the service). The operations are grouped in the following services:

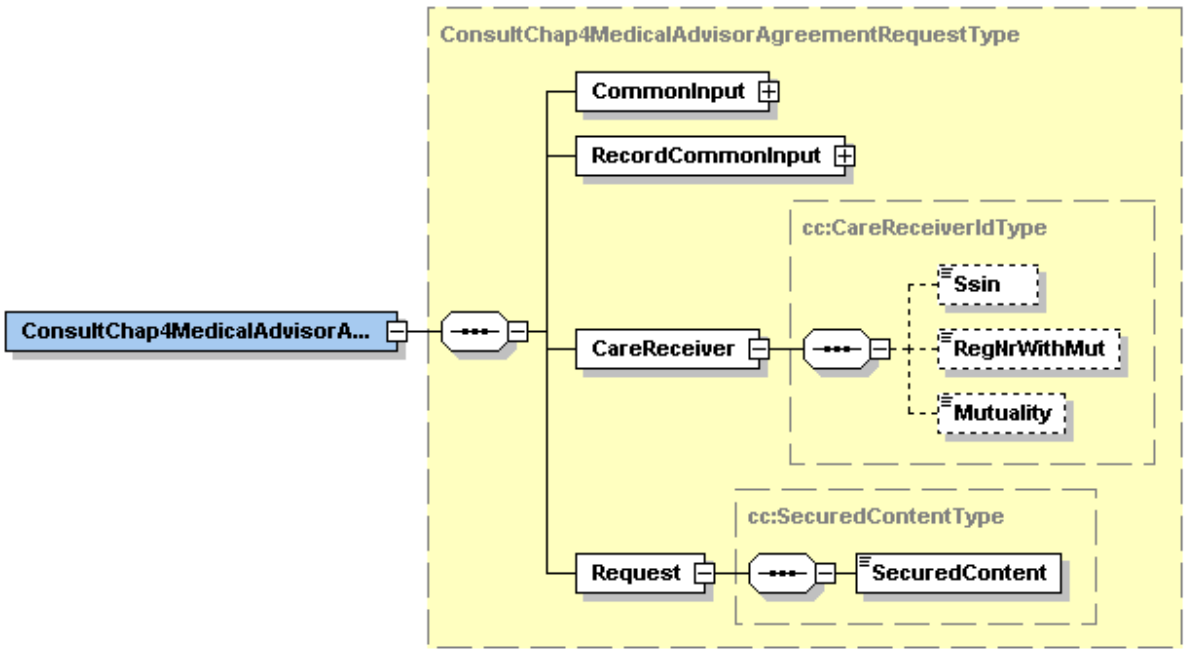
- Chap4AgreementConsultationWebservice
    - consultChap4MedicalAdvisorAgreement
- Chap4AgreementAdmissionWebservice
    - askChap4MedicalAdvisorAgreement

The remainder of this section describes the structure of the business request messages. The response messages are described in Section 5. Section 6 describes the common element types used in these structures and in the structures of the response types. For more detail on the specific elements and the concepts behind them, see the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

4.1 ConsultChap4MedicalAdvisorAgreement

This section describes only the structure of the message. For the business description, see the documentation as provided by CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)
The ConsultChap4MedicalAdvisorAgreement request has the structure as shown on the figure below:

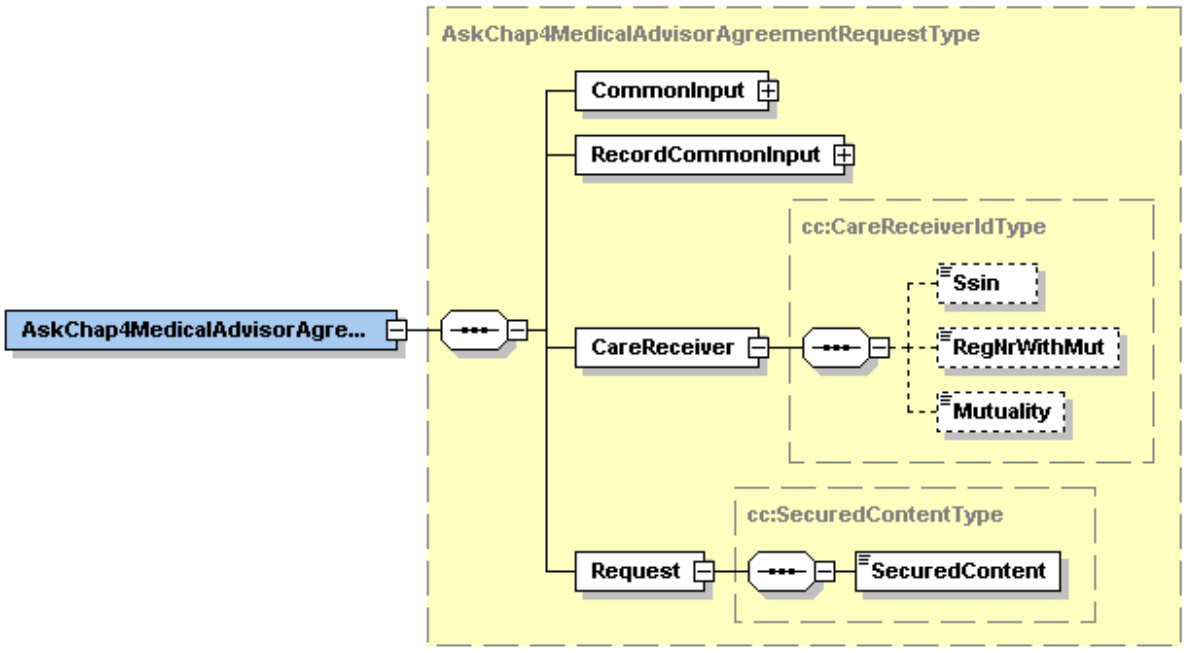
[3] WSDL's can be found in the eHealth Service Registry: https://services.ehealth.fgov.be/registry/uddi/bsc/web



Field name	Descriptions
CommonInput	See section 5.1: CommonInputType
RecordCommonInput	See section 5.2: RecordCommonInputType
CareReceiver	See the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)
Request	See the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

4.2 AskChap4MedicalAdvisorAgreement

The AskChap4MedicalAdvisorAgreement request has the structure as shown on the figure below:



Field name	Descriptions
CommonInput	See section 5.1: CommonInputType
RecordCommonInput	See section 5.2: RecordCommonInputType
CareReceiver	See the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)
Request	See the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

5 Response from the Chapter IV webservice

There are different possible types of response:

- If there are no technical errors, responses as described in the remainder of this section are returned. Section 5 describes the common element types for the responses and the requests. For more detail on the specific elements and the concepts behind them, see the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)
- In the case of a technical error, a SOAP fault exception is returned (see table 1).

Table 1: Description of the possible SOAP fault exceptions.

Code	Message
SOA-00001	Service error
SOA-01001	Service call not authenticated
SOA-01002	Service call not authorized
SOA-02001	Service temporarily not available. Please try later
SOA-02002	Message must be SOAP
SOA-03001	Malformed message
SOA-03002	Message must be SOAP
SOA-03003	Message must contain SOAP body
SOA-03004	WS-I compliance failure
SOA-03005	WSDL compliance failure
SOA-03006	XSD compliance failure
SOA-03007	Message content validation failure

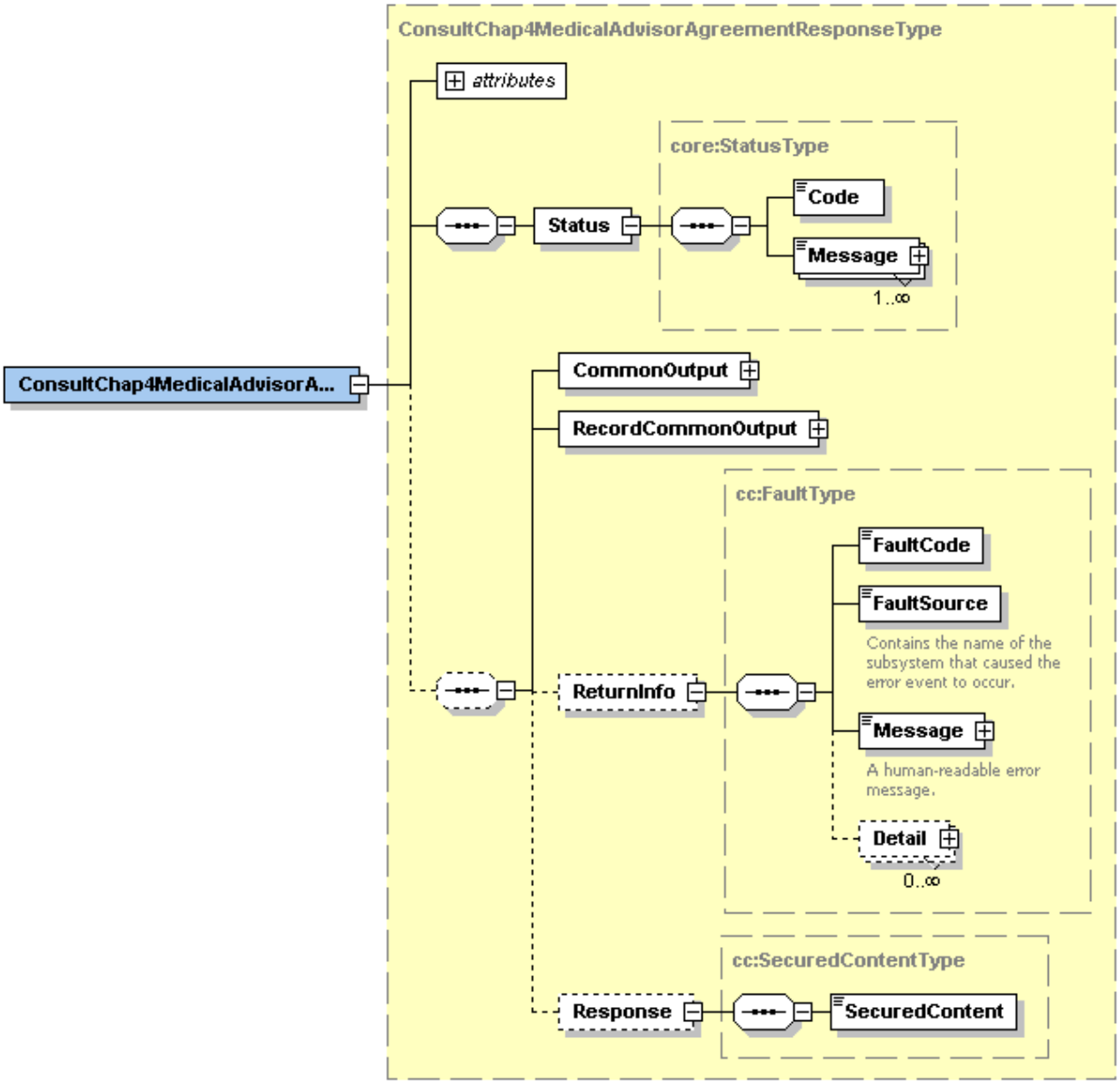
The soap header (only when the received response is not a SOAP fault) contains a message ID, e.g.:

```
<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.

5.1 ConsultChap4MedicalAdvisorAgreement

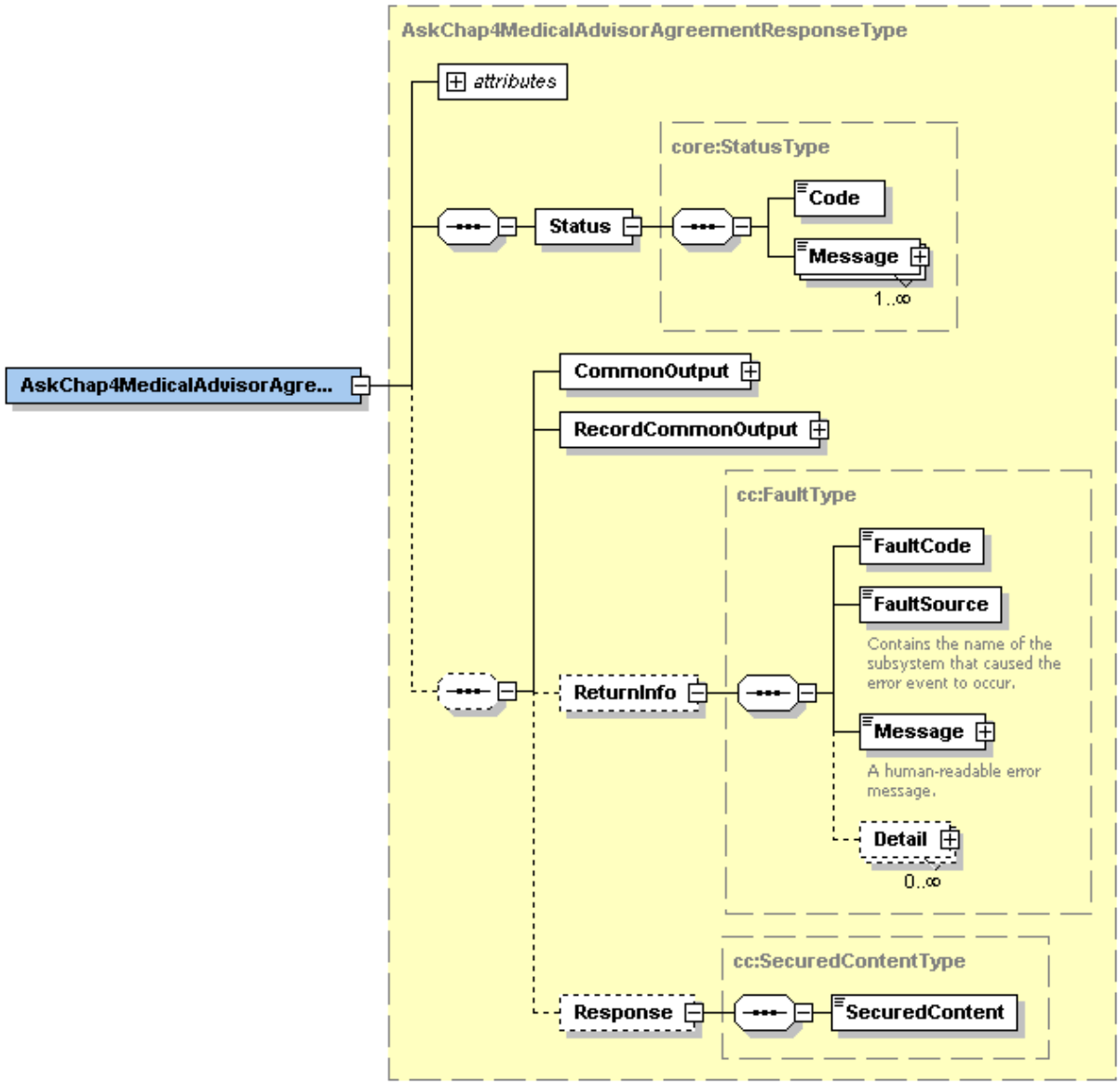
The ConsultChap4MedicalAdvisorAgreement response has the structure as shown on the figure below:



Field name	Descriptions
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 Table 1) or a business error is returned (see ReturnInfo element for more detail on the business error).
CommonOutput	See section 5.1: CommonOutputType
RecordCommonOutput	See section 5.2: RecordCommonOutputType
ReturnInfo	See the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)
Response	See the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

5.2 AskChap4MedicalAdvisorAgreement

The AskChap4MedicalAdvisorAgreementResponse response has the structure as shown on the figure below:



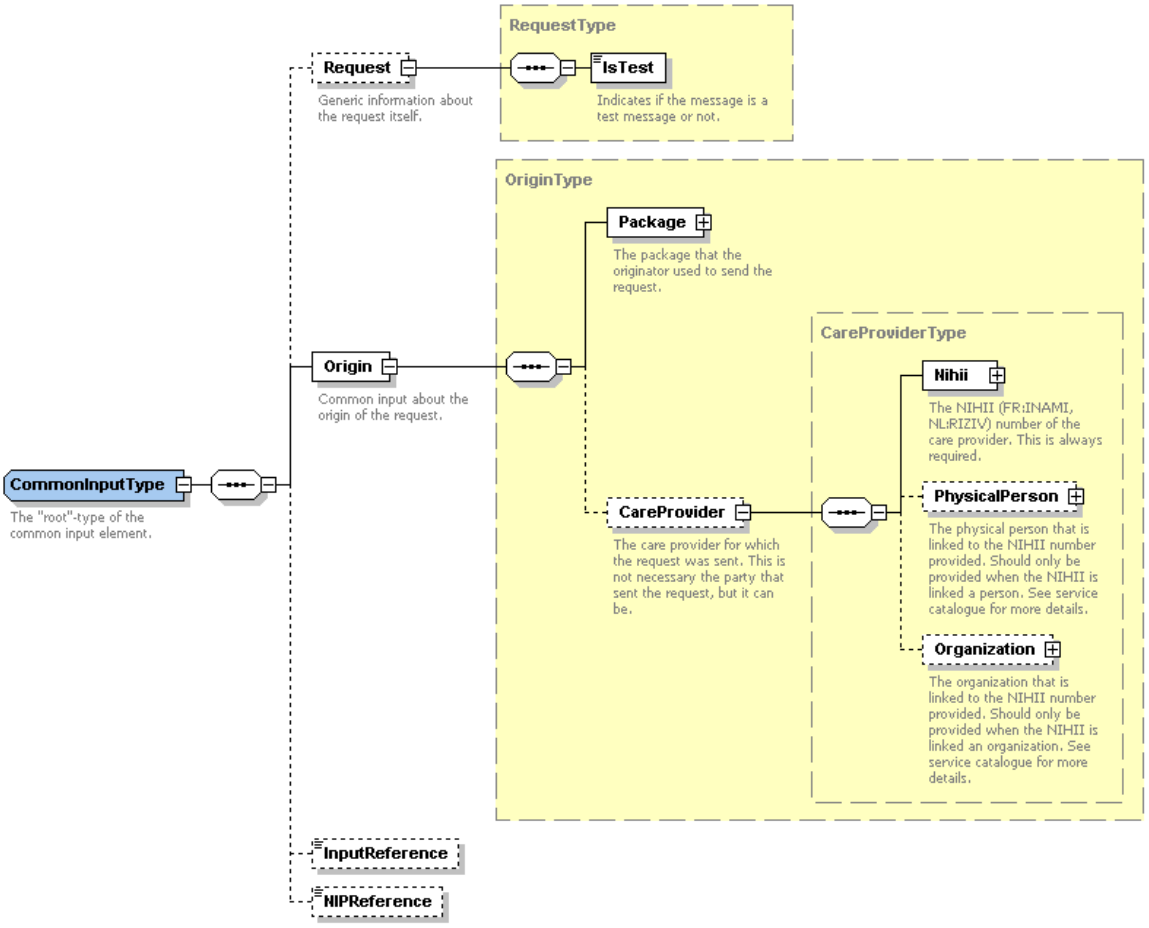
Field name	Descriptions
Status	The Status element contains a code and a message. If no error has occurred during the call, the Code is set to "200" and the Message is "Success". Otherwise, a soap fault exception is returned (see also Table 1) or a business error is returned (see ReturnInfo element for more detail on the business error).
CommonOutput	See section 5.1: CommonOutputType
RecordCommonOutput	See section 5.2: RecordCommonOutputType
ReturnInfo	See the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

Response	See the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

6 Common data structures

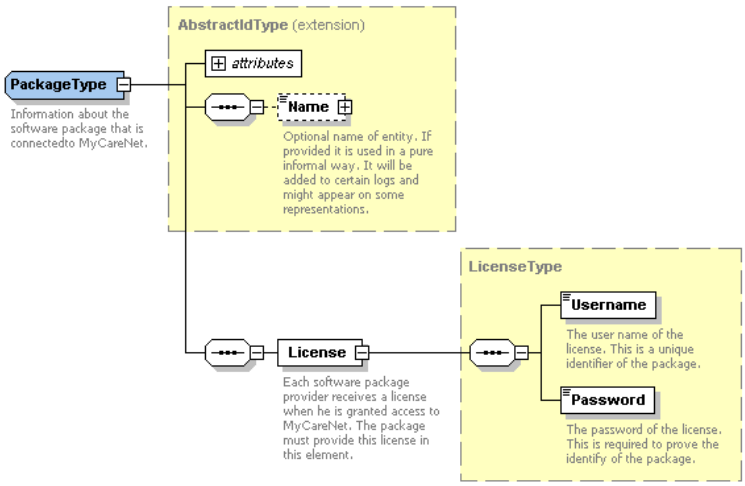
All operations reuse some of the common data structures described below.

6.1 CommonInputType



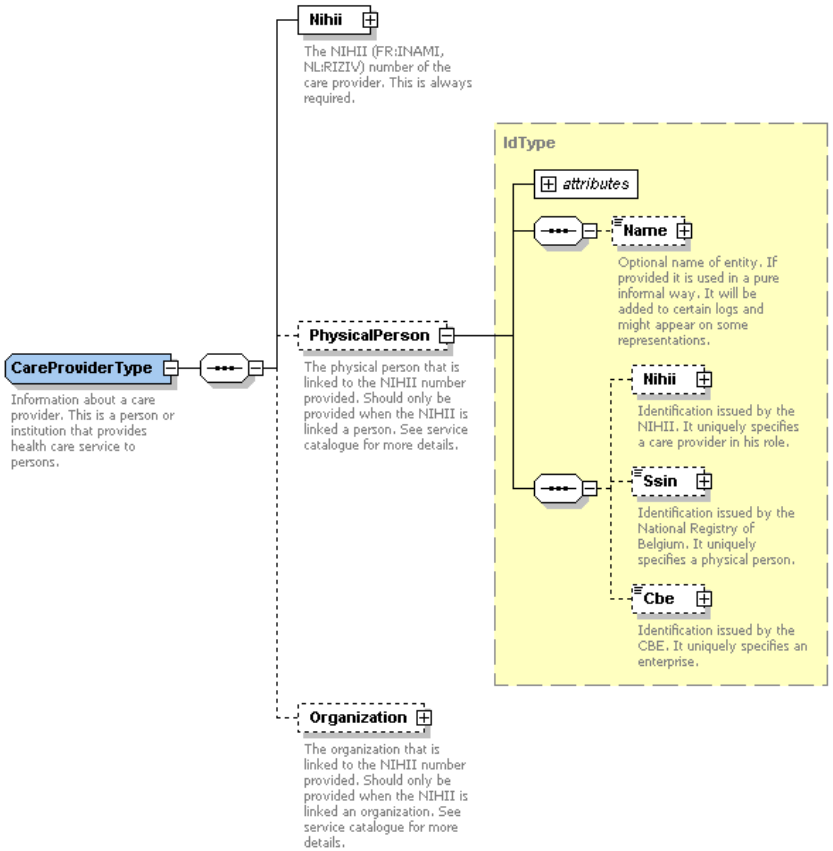
For the semantics of the particular elements and other information about the service see the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

Package:



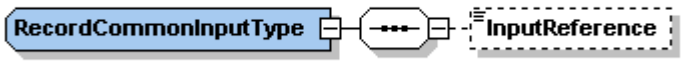
For the semantics of the particular elements and other information about the service see the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

Care Provider:



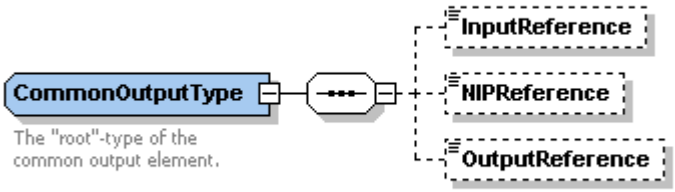
For the semantics of the particular elements see the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

6.2 RecordCommonInputType



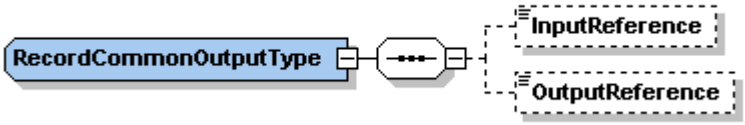
For the semantics of the particular elements see the documentation ("MyCareNet Service Catalogue", and other) as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

6.3 CommonOutputType



For the semantics of the particular elements see the as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)

6.4 RecordCommonOutputType



For the semantics of the particular elements see the documentation as provided by the CIN/NIC (see the documentation contained in the "MyCareNet functional description 01.zip" archive)