SMUREG WS SDS
Cookbook
Version 1.3

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

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 document references 5
3 Support 6
3.1 For issues in production 6
3.2 For issues in acceptance 6
3.3 For business issues 6
3.4 Certificates 6
4 Global overview 7
5 Step-by-step 8
5.1 Access to the Web Service 8
5.2 Authentication workflow 8
5.3 Technical requirements 9
5.3.1 Use of the eHealth SSO solution 9
5.3.2 Security policies to apply 10
5.3.3 WS-I Basic Profile 1.1 10
5.3.4 Tracing 10
5.4 Process overview 10
5.4.1 Web Service WSDL (Web Service Definition Language) 11
5.5 Web service 11
5.5.1 SaveIntervention Method 11
5.5.2 DeleteIntervention Method 17
5.5.3 IsAlive Method 21
5.5.4 Used Types 24
6 Risks and security 28
6.1 Security 28
6.1.1 Business security 28
6.1.2 Web service 28
6.1.3 The use of username, password and token 28
7 Test and release procedure 29

7.1 Procedure ... 29
7.1.1 Initiation ... 29
7.1.2 Development and test procedure ... 29
7.1.3 Release procedure ... 29
7.1.4 Operational follow-up ... 29
7.2 Test cases ... 29
8 Error and failure messages ... 30
8.1 SaveIntervention Response Status Codes ... 30
8.2 Soap Fault Error Codes ... 30
8.2.1 Schema Validation Errors ... 32
8.2.2 Technical Errors ... 33
9 List of sources ... 35
10 Annex 1 – Expected field values ... 36
10.1 Expected values for “originator” ... 36
10.2 Expected values for “eventNumber” ... 36
10.3 Expected values for “mobileRadio” ... 36
10.4 Expected values for “typeOfCaller” ... 37
10.5 Expected values for “interventionPlace” ... 37
10.6 Expected values for “transportCode” ... 37
10.7 Expected values for “hospitalCode” ... 38

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	20/05/2011	Stefan Dawir	Initial version
1.1	24/05/2011	Nicolas Rogge	Suppression d'une remarque
1.2	20/02/2012	Nicolas Slegers	SmuregSDSService WebService Release
1.3	06/01/2021	EMSR Team	- Following fields were added to saveIntervention: • typeSubtypeAlert • typeSubtypeAvailable • destinationHospitalOfAlertCode • destinationHospitalOfAlertCodeAs • destinationHospitalAfterInterventionCode • destinationHospitalAfterInterventionCodeAs -added the DeleteIntervention Method -changed definition of hospitalcode

2 Introduction

2.1 Goal of the service

The main goal of this service is to allow the CAD service to send CAD intervention related data into the SMUREG system that is used by SMUR, MUG and PIT to complete an intervention report through web application.

The intervention radio message provided by CAD service is substantial information that is meant to be the reference for timing and geolocation information in an intervention report.

Thus it will be possible:

- To know the exact timings for intervention and to rely on them for statistics later.
- Reduce the amount of information to be submitted by the administrative staff to record an intervention file.
- Make available the information that hospitals do not yet have it in their system.

2.2 Goal of the document

This document is not a development or programming guide for internal applications. Instead it provides functional and technical information and allows an organization to integrate and use the eHealth service.

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

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

2.3 eHealth document references

All the document references can be found in the technical library 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
2	Cookbook STS	1.4	24/02/2021	eHealth
3	Interface Control Document – CAD2MUREG	2.4	1/08/2011	Intergraph

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

3 Support

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

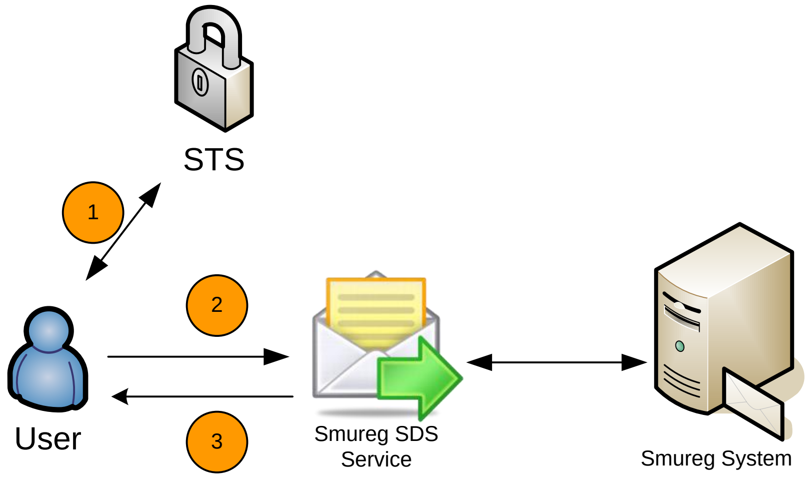
  https://www.ehealth.fgov.be/ehealthplatform/fr/certificats-ehealth

- For technical issues regarding eHealth platform certificates

  Acceptance: ***acceptance-certificates@ehealth.fgov.be***

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

4 Global overview



This global overview aims to show how the SMUREG SDS web service is used.

1. To use the SMUREG SDS web service, you have to contact the web service STS to get a secure token containing the identification of the user.
2. Once your token returned, you are able to use and contact the SMUREG SDS web service to send your SDS message.
3. When your SDS message has been sent, the system will respond you with an acknowledgement message.

5 Step-by-step

5.1 Access to the Web Service

For each web service accessed on eHealth platform, authentication ensures that the requester is allowed. eHealth certificates are used to trust the requester and provide some information like the organization type, the INAMI number, and so on… A Web Service named STS has to be call with specific parameters to generate an assertion which will enrich the eHealth certificate.

Thus, when calling the SMUREG SDS Web Service, eHealth intercepts the request to check and validate the certificate and then dispatch it to the Web Service; if additional information garnishes the request, they will be used by the web service to check additional constraints.

The documentation regarding STS can be found at: (documents are in English)

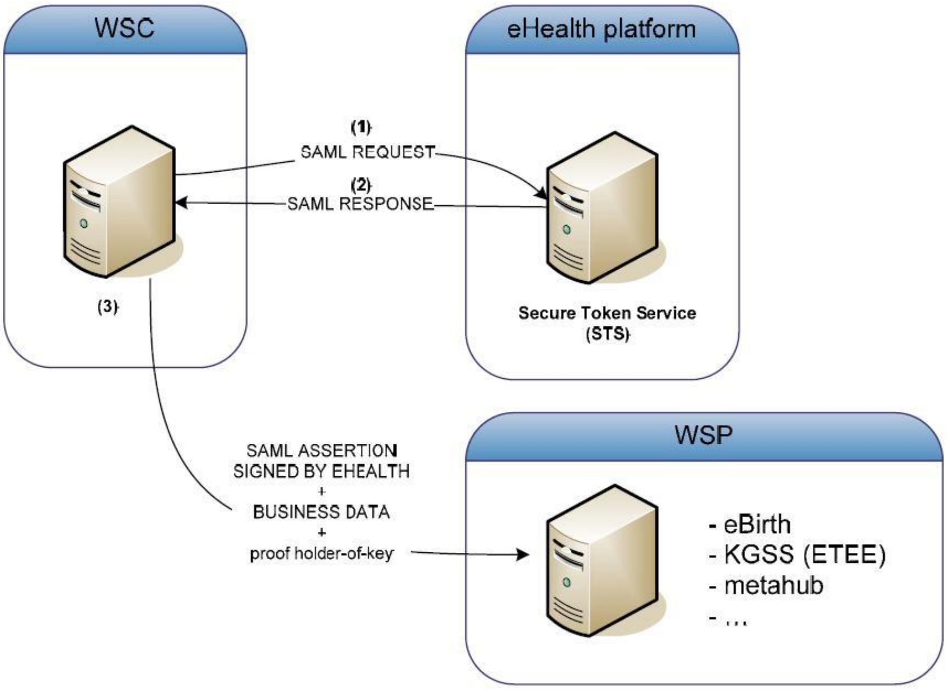
- Secure Token Service - HolderofKey - Cookbook (F)
- Secure Token Service - HolderofKey - Cookbook (Nl)

In order to access STS, requestors must prove their identity by using one of the following certificates:

- An eHealth certificate. This is used to identify the initiator of the request.
- A Belgian Electronic Identity Card (eID) with a supported card reader

5.2 Authentication workflow

The following figure illustrates how the different calls are performed. Notice that the session ticket generated can be valid for a maximum of 24 hours duration.



Web service consumer authenticates with the STS (using the eHealth certificate) in order to obtain a session ticket (SAML token) that is then used in calls to the provider.

The provider verifies the authenticity of the SAML assertion by checking the signature of the STS. The provider also checks that the consumer is the lawful owner of the SAML assertion by verifying the signature of the consumer.
Holder-of-Key is the standard policy for the spread of identity when consumers outside Smals network must authenticate using a SAML assertion.

1. A request containing an X.509 certificate (eHealth certificate) is sent to STS by the consumer to obtain a SAML token. The body of the message and the security token must be signed to ensure authenticity and integrity.
   The request must contain the information that eHealth must validate (to be defined with eHealth and the requestors).
2. eHealth STS Web Service sends a signed SAML assertion to the client with the message containing the information confirmed (Proof of authentication).
3. The token obtained has a duration of validity, specified in the token, and can be reused for all requests to the SMUREG SDS web service.
4. The request to SMUREG SDS web service is created with the SAML token in header.
5. The answer to the request is transmitted to the client.

5.3 Technical requirements

5.3.1 Use of the eHealth SSO solution

The complete overview of the profile and a step-by-step description of how to protect a new application with the SSO @ eHealth are described in the eHealth SSO cookbook.

This section specifies how to obtain a SAML token from the STS (Secure Token Service) in order to have access to the web service. There are different types of users; 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.

The request for the SAML token is secured with the certificate of a 100 central. The certificate used by the Holder-Of-Key verification mechanism is an eHealth certificate. The needed attributes are the following (AttributeNamespace: "urn:be:fgov:identification-namespace"):

- The EHP number of the central:
  - *urn:be:fgov:ehealth:1.0:certificateholder:organization:ehp-number* and *urn:be:fgov:ehealth:1.0:100central:ehp-number*

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

- The organization EHP number
  - *urn:be:fgov:ehealth:1.0:certificateholder:organization:ehp-number*
  - *(namespace :* urn:be:fgov:identification-namespace)
  - *urn:be:fgov:ehealth:1.0:100central:ehp-number*
  - *(namespace :* urn:be:fgov:identification-namespace)
- To have access to the service, identifier must be a recognised 100 central
  - *urn:be:fgov:ehealth:1.0:certificateholder:organization:ehp-number:recognised100central:boolean*
  - (namespace : urn:be:fgov:certified-namespace:ehealth)

5.3.2 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 doesn't arrive during this minute, he 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 will allow eHealth to verify the integrity of the message and the identity of the message author.

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

The STS cookbook can be found on the eHealth portal. [2]

5.3.3 WS-I Basic Profile 1.1

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

5.3.4 Tracing

To use this service, the request SHOULD contain the following two http header values (see RFC ***https://www.w3.org/Protocols/rfc2616/rfc2616-sec3.html#sec3.8***):

1. **User-Agent**: information identifying the software product and underlying technical stack/platform.

   - Pattern: {company}/{package-name}/{version} {platform-company}/{platform-package-name}/{platform-package-version}
   - Regular expression for each subset (separated by a space) of the pattern: [[a-zA-Z0-9-\/]*\/[0-9a-zA-Z-_.]*
   - Examples:
     User-Agent: MyCompany/myProduct/62.310.4 eHealth/Technical/3.19.0
     User-Agent: Topaz-XXXX/123.23.X Taktik/freeconnector/XXXXX.XXX

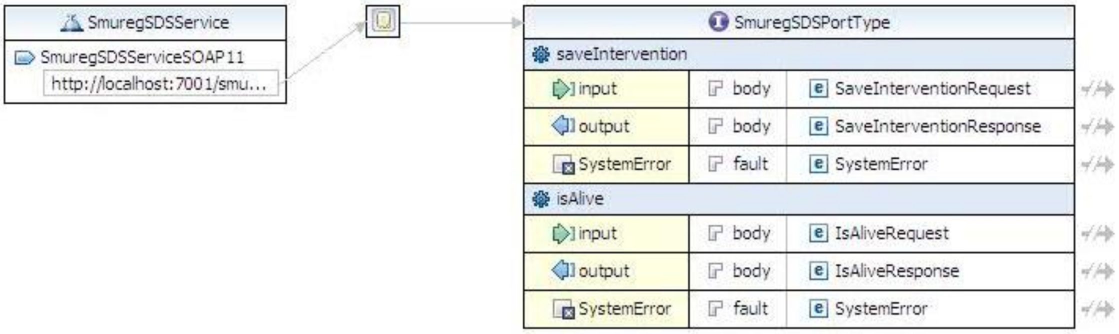
2. **From:** email-address that can be used for emergency contact in case of an operational problem
   Examples:
   From: *info@mycompany.be*

5.4 Process overview

All the xml requests submitted to the web service must be encoded in the UTF-8 format.

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

5.4.1 Web Service WSDL (Web Service Definition Language)



SmuregSDSService

SmuregSDSServiceSOAP11

http://localhost:7001/smu...

SmuregSDSPortType		
saveIntervention		
input	body	SaveInterventionRequest
output	body	SaveInterventionResponse
SystemError	fault	SystemError
isAlive		
input	body	IsAliveRequest
output	body	IsAliveResponse
SystemError	fault	SystemError

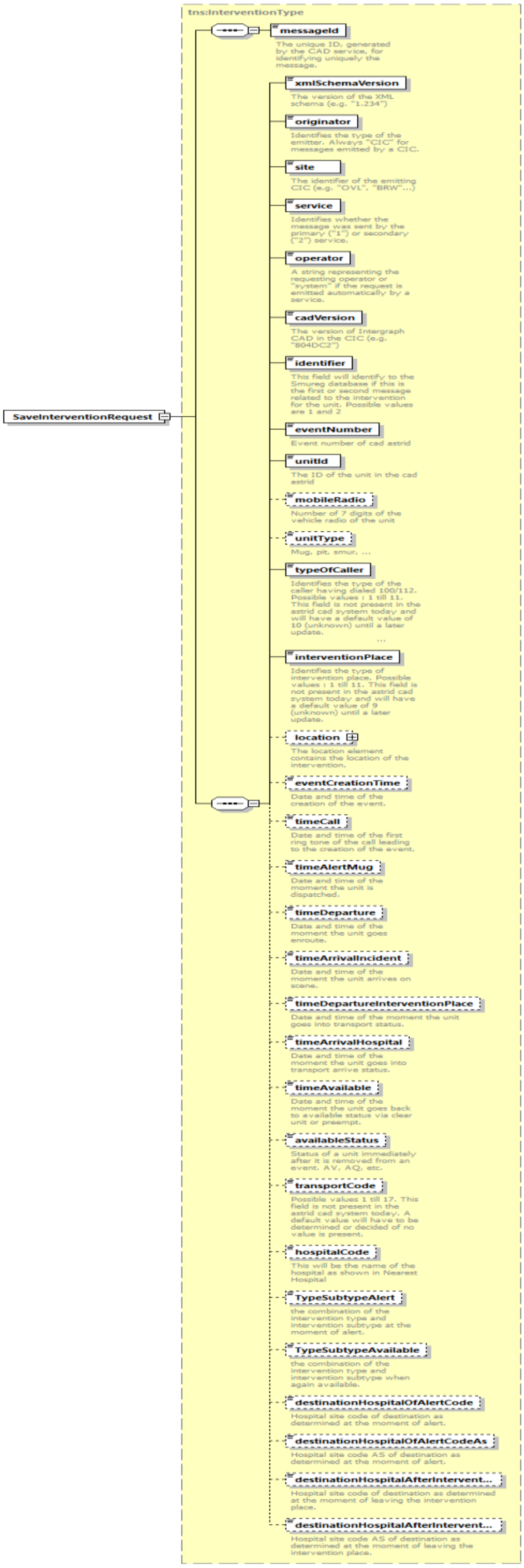
5.5 Web service

5.5.1 SaveIntervention Method

This method saves the intervention information sent by CAD service.

The expected field values are listed in Annex 1 – Expected field values. SMUREG will not be able to treat any other values received. Changes can be made in agreement with eHealth.

5.5.1.1 SaveIntervention Request



messageId
The unique ID, generated by the CAD service, for identifying uniquely the message.

xmlSchemaVersion
The version of the XML schema (e.g. "1.234")

originator
Identifies the type of the emitter. Always "CIC" for messages emitted by a CIC.

site
The identifier of the emitting CIC (e.g. "OVL", "BRW"...)

service
Identifies whether the message was sent by the primary ("1") or secondary ("2") service.

operator
A string representing the requesting operator or "system" if the request is emitted automatically by a service.

cadVersion
The version of Intergraph CAD in the CIC (e.g. "804DC2")

identifier
This field will identify to the Smureg database if this is the first or second message related to the intervention for the unit. Possible values are 1 and 2

eventNumber
Event number of cad astrid

unitId
The ID of the unit in the cad astrid

mobileRadio
Number of 7 digits of the vehicle radio of the unit

unitType
Mug, pit, smur, ...

typeOfCaller
Identifies the type of the caller having dialed 100/112. Possible values : 1 till 11. This field is not present in the astrid cad system today and will have a default value of 10 (unknown) until a later update.
...

interventionPlace
Identifies the type of intervention place. Possible values : 1 till 11. This field is not present in the astrid cad system today and will have a default value of 9 (unknown) until a later update.

location
The location element contains the location of the intervention.

eventCreationTime
Date and time of the creation of the event.

timeCall
Date and time of the first ring tone of the call leading to the creation of the event.

timeAlertMug
Date and time of the moment the unit is dispatched.

timeDeparture
Date and time of the moment the unit goes enroute.

timeArrivalIncident
Date and time of the moment the unit arrives on scene.

timeDepartureInterventionPlace
Date and time of the moment the unit goes into transport status.

timeArrivalHospital
Date and time of the moment the unit goes into transport arrive status.

timeAvailable
Date and time of the moment the unit goes back to available status via clear unit or preempt.

availableStatus
Status of a unit immediately after it is removed from an event. AV, AQ, etc.

transportCode
Possible values 1 till 17. This field is not present in the astrid cad system today. A default value will have to be determined or decided of no value is present.

hospitalCode
This will be the name of the hospital as shown in Nearest Hospital

TypeSubtypeAlert
the combination of the intervention type and intervention subtype at the moment of alert.

TypeSubtypeAvailable
the combination of the intervention type and intervention subtype when again available.

destinationHospitalOfAlertCode
Hospital site code of destination as determined at the moment of alert.

destinationHospitalOfAlertCodeAs
Hospital site code AS of destination as determined at the moment of alert.

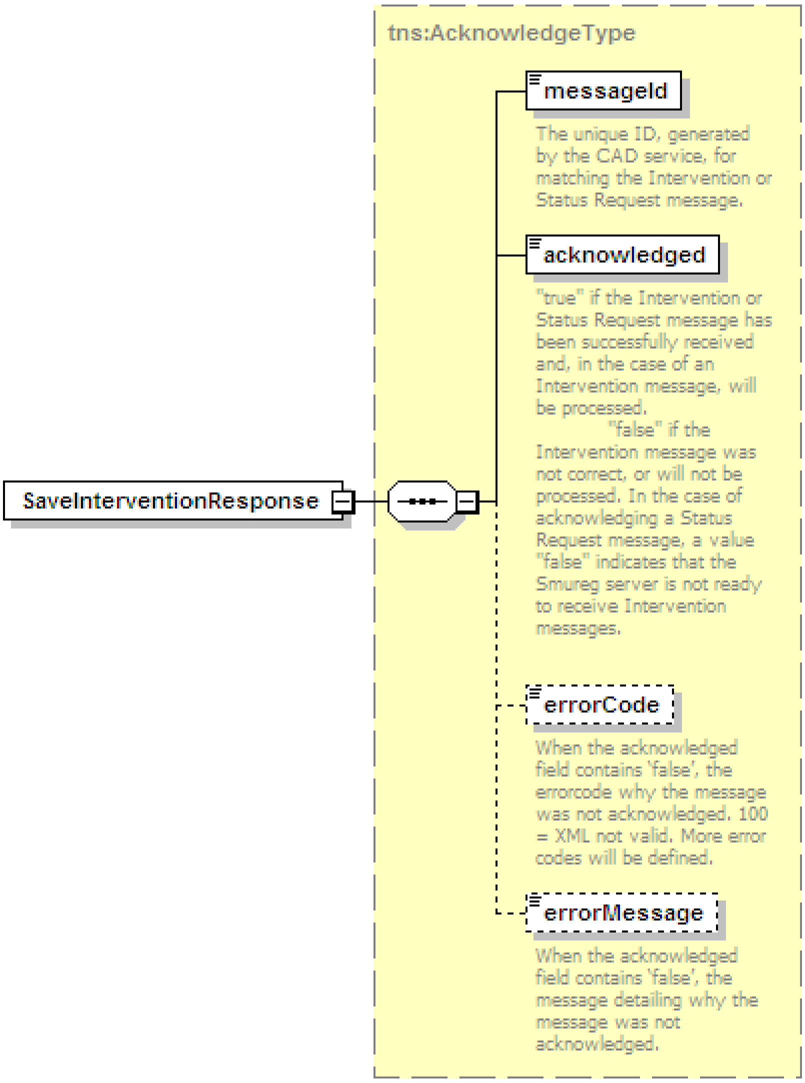
destinationHospitalAfterIntervent...
Hospital site code of destination as determined at the moment of leaving the intervention place.

destinationHospitalAfterIntervent...
Hospital site code AS of destination as determined at the moment of leaving the intervention place.

	Description	Mandatory
messageId	The unique ID, generated by the CAD service, for identifying uniquely the message.	yes
xmlSchemaVersion	The version of the XML schema (e.g. "1.234")	Yes
originator	Identifies the type of the emitter. "CIC" for InterGraph or “C100” for CityGIS.	Yes
site	The identifier of the emitting CIC (e.g. "OVL", "BRW"...)	Yes
service	Identifies whether the message was sent by the primary ("1") or secondary ("2") service.	Yes
operator	A string representing the requesting operator or "system" if the request is emitted automatically by a service.	Yes
cadVersion	The version of Intergraph CAD in the CIC (e.g. "804DC2")	Yes
identifier	This field will identify to the SMUREG database if this is the first or second message related to the intervention for the unit. Possible values are 1 and 2	Yes
eventNumber	Event number of CAD astrid	Yes
unitId	The ID of the unit in the CAD astrid	Yes
mobileRadio	Number of 7 digits of the vehicle radio of the unit	No
unitType	Mug, pit, smur, ...	No
typeOfCaller	Identifies the type of the caller having dialed 100/112. Possible values: 1 till 11.	Yes
interventionPlace	Identifies the type of intervention place. Possible values: 1 till 11. This field is not present in the astrid CAD system today and will have a default value of 9 (unknown) until a later update.	Yes
location	The location element contains the location of the intervention.	No
eventCreationTime	Date and time of the creation of the event.	No
timeCall	Date and time of the first ring tone of the call leading to the creation of the event.	No
timeAlertMug	Date and time of the moment the unit is dispatched.	No
timeDeparture	Date and time of the moment the unit goes enroute.	No

timeArrivalIncident	Date and time of the moment the unit arrives on scene.	No
timeDepartureInterventionPlace	Date and time of the moment the unit goes into transport status.	No
timeArrivalHospital	Date and time of the moment the unit goes into transport arrive status.	No
timeAvailable	Date and time of the moment the unit goes back to available status via clear unit or preempts.	No
availableStatus	Status of a unit immediately after it is removed from an event. AV, AQ, etc.	No
transportCode	Possible values 1 till 17. This field is not present in the astrid CAD system today. A default value will have to be determined or decided of no value is present.	No
hospitalCode	Not used anymore, replaced by destinationHospitalOfAlertCode, destinationHospitalOfAlertCodeAs, destinationHospitalAfterInterventionCode and destinationHospitalAfterInterventionCodeAs	No
typeSubtypeAlert	The combination of the intervention type and intervention subtype at the moment of alert as a code of 7 numbers with format 6 IT ST 01 with IT standing for the intervention type between 01 and 99 and with ST standing for the intervention subtype between 01 and 27.	No
typeSubtypeAvailable	the combination of the intervention type and intervention subtype when again available.	No
destinationHospitalOfAlertCode	Hospital site code of destination as determined at the moment of alert. The values are published by the SPF Health.	No
destinationHospitalOfAlertCodeAs	Hospital site code AS of destination as determined at the moment of alert. The values are published by the SPF Health.	No
destinationHospitalAfterInterventionCode	Hospital site code of destination as determined at the moment of leaving the intervention place. The values are published by the SPF Health.	No
destinationHospitalAfterInterventionCodeAs	Hospital site code AS of destination as determined at the moment of leaving the intervention place. The values are published by the SPF Health.	No

5.5.1.2 SaveIntervention Response


tns:AcknowledgeType
messageId
The unique ID, generated by the CAD service, for matching the Intervention or Status Request message.
acknowledged
"true" if the Intervention or Status Request message has been successfully received and, in the case of an Intervention message, will be processed. "false" if the Intervention message was not correct, or will not be processed. In the case of acknowledging a Status Request message, a value "false" indicates that the Smureg server is not ready to receive Intervention messages.
errorCode
When the acknowledged field contains 'false', the errorcode why the message was not acknowledged. 100 = XML not valid. More error codes will be defined.
errorMessage
When the acknowledged field contains 'false', the message detailing why the message was not acknowledged.
SaveInterventionResponse

Field name	Description
messageId	The unique ID, generated by the CAD service, for matching the Intervention or Status Request message.
acknowledged	"true" if the Intervention or Status Request message has been successfully received and, in the case of an Intervention message, will be processed. "false" if the Intervention message was not correct, or will not be processed. In the case of acknowledging a Status Request message, a value "false" indicates that the SMUREG server is not ready to receive Intervention messages.
errorCode	When the acknowledged field contains 'false', the error code why the message was not acknowledged. 100 = XML not valid. More error codes will be defined.
errorMessage	When the acknowledged field contains 'false', the message detailing why the message was not acknowledged.

5.5.1.3 Example

The following example does not contain the SAML assertion.

Request:

```xml
<tns:SaveInterventionRequest xsi:schemaLocation="urn:be:fgov:ehealth:smuregsdsws:protocol:v1 smureg_sds_protocol_v1_0.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:tns="urn:be:fgov:ehealth:smuregsdsws:protocol:v1">

    <messageId>798</messageId>

    <xmlSchemaVersion>1.1</xmlSchemaVersion>

    <originator>CIC</originator>

    <site>NAM</site>

    <service>1</service>

    <operator>system</operator>

    <cadVersion>804DC4</cadVersion>

    <identifier>1</identifier>

    <eventNumber>fh00000024</eventNumber>

    <unitId>GENT202</unitId>

    <mobileRadio>8000007</mobileRadio>

    <unitType>smur</unitType>

    <typeOfCaller>10</typeOfCaller>

    <interventionPlace>9</interventionPlace>

    <location>

        <longitude>4.351694</longitude>

        <latitude>50.850437</latitude>

        <commonPlace>delhaize</commonPlace>

        <street1>

            <name>kerkstraat</name>

            <number>17</number>

            <area>1030</area>

            <municipality>brussel</municipality>

            <apartment>String</apartment>

        </street1>

        <street2>

            <name>String</name>

            <number>String</number>
            <area>String</area>
            <municipality>String</municipality>
            <apartment>String</apartment>
            <field1>String</field1>
            <field2>String</field2>
            <field3>String</field3>
        </street2>
    </location>
    <eventCreationTime>2011-04-21T15:47:11</eventCreationTime>
    <timeCall>2011-04-21T15:45:12</timeCall>
    <timeAlertMug>2011-04-21T15:49:02</timeAlertMug>
    <timeDeparture>2011-04-21T15:52:37</timeDeparture>
    <timeArrivalIncident>2011-04-21T15:59:41</timeArrivalIncident>
    <timeDepartureInterventionPlace>2011-04-
21T16:17:07</timeDepartureInterventionPlace>
    <timeArrivalHospital>2011-04-21T16:25:26</timeArrivalHospital>
    <timeAvailable>2011-04-21T16:40:20</timeAvailable>
    <availableStatus>av</availableStatus>
    <transportCode>15</transportCode>
    <hospitalCode>Hôpital de la Meuse</hospitalCode>
</tns:SaveInterventionRequest>
```

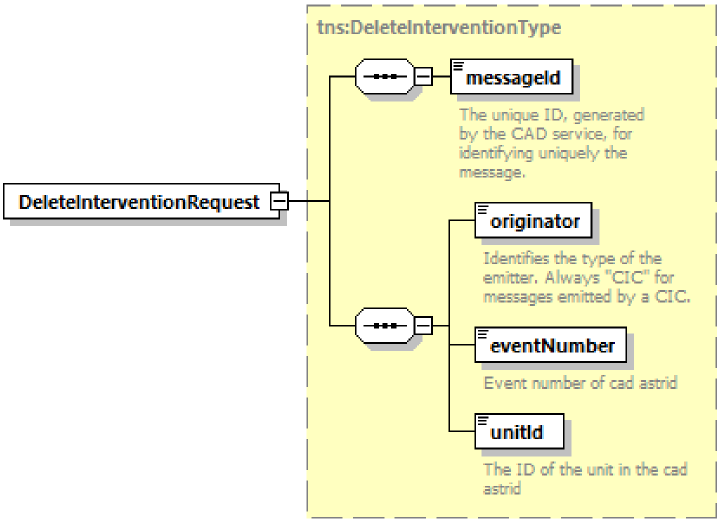
Response:

```
<tns:SaveInterventionResponse xsi:schemaLocation="urn:be:fgov:ehealth:smuregsd
sws:protocol:v1 smureg_sds_protocol_v1_0.xsd" xmlns:xsi="http://www.w3.org/200
1/XMLSchema-instance" xmlns:tns="urn:be:fgov:ehealth:smuregsdsws:protocol:v1">
    <messageId>112233</messageId>
    <acknowledged>true</acknowledged>
</tns:SaveInterventionResponse>
```

5.5.2 DeleteIntervention Method

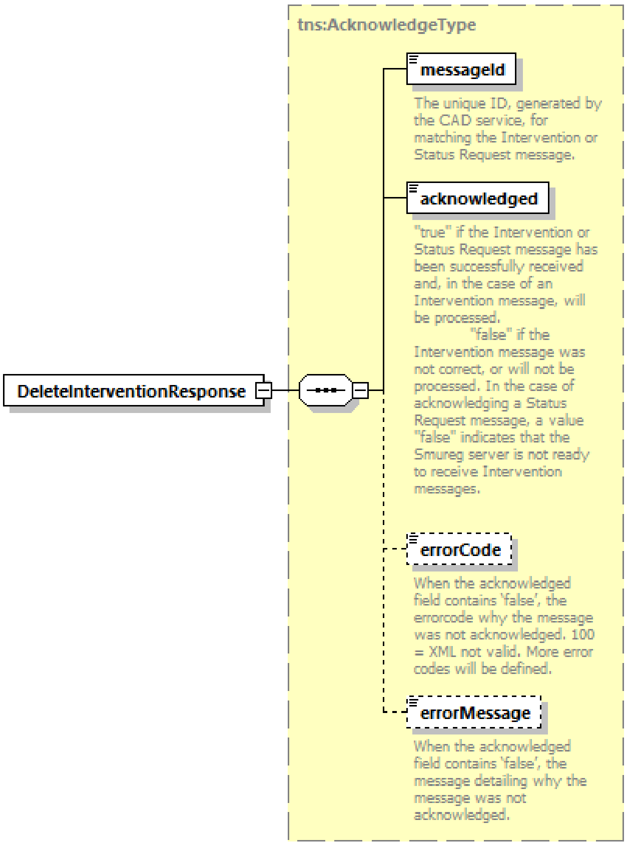
This method deletes all alerts linked to an event number.

5.5.2.1 DeleteIntervention Request


tns:DeleteInterventionType
DeleteInterventionRequest
messageId
The unique ID, generated by the CAD service, for identifying uniquely the message.
originator
Identifies the type of the emitter. Always "CIC" for messages emitted by a CIC.
eventNumber
Event number of cad astrid
unitId
The ID of the unit in the cad astrid

Field name	Description	Mandatory
messageId	The unique ID, generated by the CAD service, for matching the Intervention or Status Request message.	Yes
originator	Identifies the type of the emitter. Always "CIC" for messages emitted by a CIC.	Yes
eventNumber	Event number of CAD astrid	Yes
unitId	The ID of the unit in the CAD astrid	Yes

5.5.2.2 DeleteIntervention Response


tns:AcknowledgeType
messageId
The unique ID, generated by the CAD service, for matching the Intervention or Status Request message.
acknowledged
"true" if the Intervention or Status Request message has been successfully received and, in the case of an Intervention message, will be processed. "false" if the Intervention message was not correct, or will not be processed. In the case of acknowledging a Status Request message, a value "false" indicates that the Smureg server is not ready to receive Intervention messages.
errorCode
When the acknowledged field contains 'false', the errorcode why the message was not acknowledged. 100 = XML not valid. More error codes will be defined.
errorMessage
When the acknowledged field contains 'false', the message detailing why the message was not acknowledged.
DeleteInterventionResponse

Field name	Description
messageId	The unique ID, generated by the CAD service, for matching the Intervention or Status Request message.
acknowledged	"true" if the Intervention or Status Request message has been successfully received and, in the case of an Intervention message, will be processed. "false" if the Intervention message was not correct, or will not be processed. In the case of acknowledging a Status Request message, a value "false" indicates that the SMUREG server is not ready to receive Intervention messages.
errorCode	When the acknowledged field contains 'false', the error code why the message has not been acknowledged. 100 = XML not valid. More error codes will be defined.
errorMessage	When the acknowledged field contains 'false', the message detailing why the message was not acknowledged.

5.5.2.3 Example

The following example does not contain the SAML assertion.

Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xm
lns:urn="urn:be:fgov:ehealth:smuregsdsws:protocol:v1">
```

```
   <soapenv:Header/>
   <soapenv:Body>
        <urn:DeleteInterventionRequest>
         <messageId>125</messageId>
         <originator>C100</originator>
         <eventNumber>10203430224</eventNumber>
         <unitId>MLHASJ101</unitId>
      </urn:DeleteInterventionRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

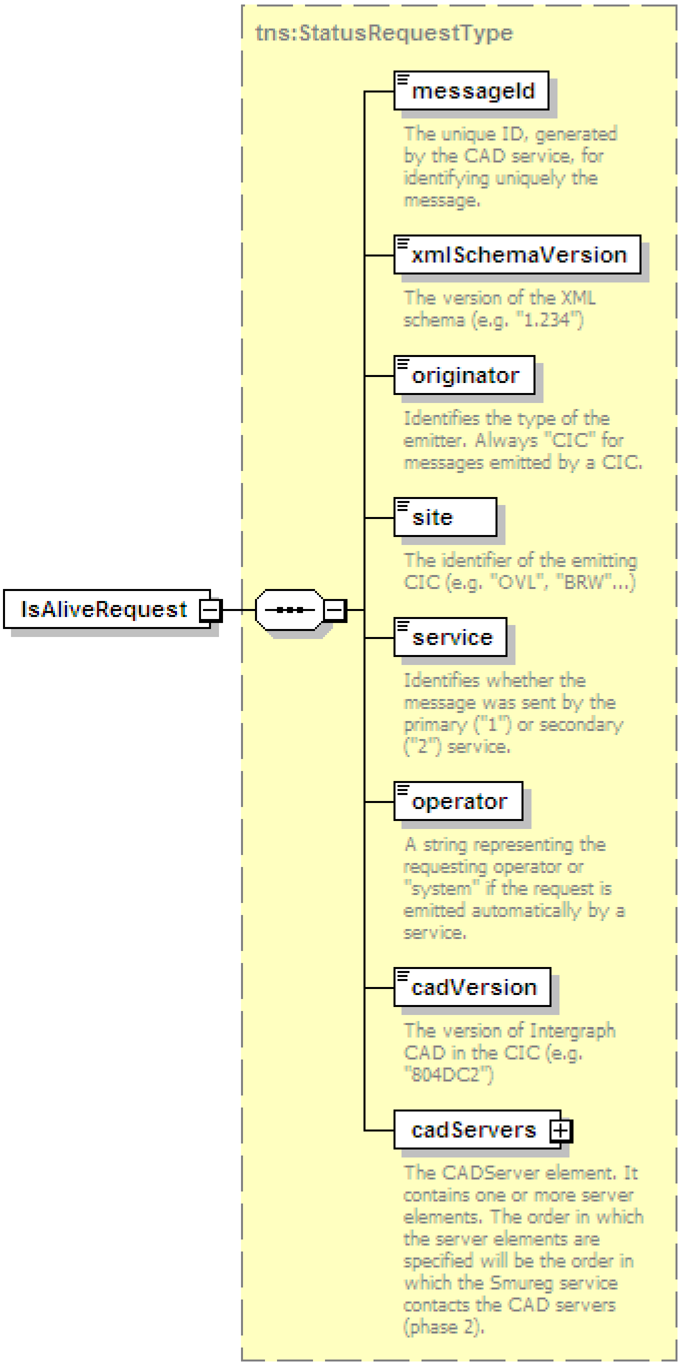
Response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
   <soap:Body>
      <ns4:DeleteInterventionResponse xmlns:ns4="urn:be:fgov:ehealth:smuregsdsws:protocol:v1" xmlns:ns3="urn:be:fgov:ehealth:errors:service:v1">
         <messageId>125</messageId>
         <acknowledged>true</acknowledged>
      </ns4:DeleteInterventionResponse>
   </soap:Body>
</soap:Envelope>
```

5.5.3 IsAlive Method

This method returns the status of the service.

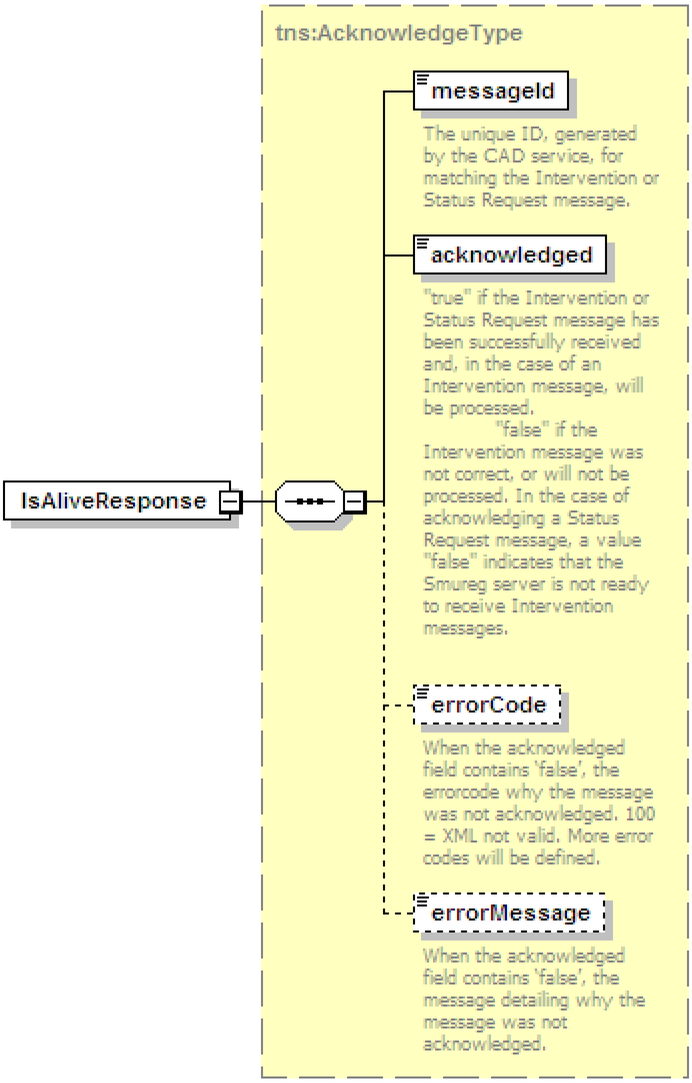
5.5.3.1 IsAlive Request


tns:StatusRequestType
IsAliveRequest
messageId
The unique ID, generated by the CAD service, for identifying uniquely the message.
xmlSchemaVersion
The version of the XML schema (e.g. "1.234")
originator
Identifies the type of the emitter. Always "CIC" for messages emitted by a CIC.
site
The identifier of the emitting CIC (e.g. "OVL", "BRW"...)
service
Identifies whether the message was sent by the primary ("1") or secondary ("2") service.
operator
A string representing the requesting operator or "system" if the request is emitted automatically by a service.
cadVersion
The version of Intergraph CAD in the CIC (e.g. "804DC2")
cadServers
The CADServer element. It contains one or more server elements. The order in which the server elements are specified will be the order in which the Smureg service contacts the CAD servers (phase 2).

Field name	Description
messageId	The unique ID, generated by the CAD service, for matching the Intervention or Status Request message.

xmlSchemaVersion	The version of the XML schema (e.g. "1.234")
originator	Identifies the type of the emitter. Always "CIC" for messages emitted by a CIC.
site	The identifier of the emitting CIC (e.g. "OVL", "BRW"...)
service	Identifies whether the message was sent by the primary ("1") or secondary ("2") service.
operator	A string representing the requesting operator or "system" if the request is emitted automatically by a service.
cadVersion	The version of Intergraph CAD in the CIC (e.g. "804DC2")
cadServers	The CADServer element. It contains one or more server elements. The order in which the server elements are specified will be the order in which the SMUREG service contacts the CAD servers (phase 2).

5.5.3.2 IsAlive Response


tns:AcknowledgeType
messageId
The unique ID, generated by the CAD service, for matching the Intervention or Status Request message.
acknowledged
"true" if the Intervention or Status Request message has been successfully received and, in the case of an Intervention message, will be processed.
"false" if the Intervention message was not correct, or will not be processed. In the case of acknowledging a Status Request message, a value "false" indicates that the Smureg server is not ready to receive Intervention messages.
IsAliveResponse
errorCode
When the acknowledged field contains 'false', the errorcode why the message was not acknowledged. 100 = XML not valid. More error codes will be defined.
errorMessage
When the acknowledged field contains 'false', the message detailing why the message was not acknowledged.

Field name	Description
messageId	The unique ID, generated by the CAD service, for matching the Intervention or Status Request message.
acknowledged	"true" if the Intervention or Status Request message has been successfully received and, in the case of an Intervention message, will be processed. "false" if the Intervention message was not correct, or will not be processed. In the case of acknowledging a Status Request message, a value "false" indicates that the SMUREG server is not ready to receive Intervention messages.
errorCode	When the acknowledged field contains 'false', the errorcode why the message was not acknowledged. 100 = XML not valid. More error codes will be defined.
errorMessage	When the acknowledged field contains 'false', the message detailing why the message was not acknowledged.

5.5.3.3 *Example*

The following example does not contain the SAML assertion.

Request:

```
<tns:IsAliveRequest xsi:schemaLocation="urn:be:fgov:ehealth:smuregsdsws:protocol:v1 smureg_sds_protocol_v1_0.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:tns="urn:be:fgov:ehealth:smuregsdsws:protocol:v1">

    <messageId>34567</messageId>

    <xmlSchemaVersion>1.1</xmlSchemaVersion>

    <originator>CIC</originator>

    <site>NAM</site>

    <service>1</service>

    <operator>system</operator>

    <cadVersion>804DC4</cadVersion>

    <cadServers>

        <server>

            <host>primary_cad</host>

            <port>50001</port>

        </server>

    </cadServers>

</tns:IsAliveRequest>
```

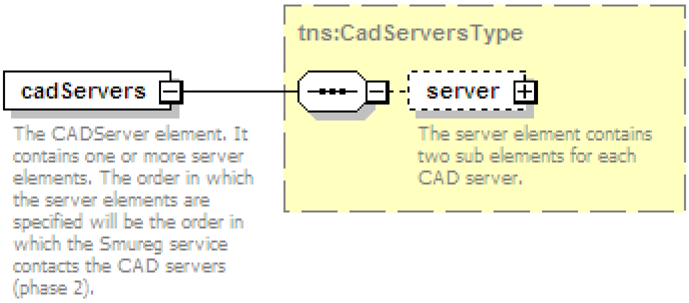
response:

```xml
<tns:IsAliveResponse xsi:schemaLocation="urn:be:fgov:ehealth:smuregsdsws:protocol:v1 smureg_sds_protocol_v1_0.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:tns="urn:be:fgov:ehealth:smuregsdsws:protocol:v1">
    <messageId>112233</messageId>
    <acknowledged>false</acknowledged>
    <errorCode>100</errorCode>
    <errorMessage>location out of Belgium</errorMessage>
</tns:IsAliveResponse>
```

5.5.4 Used Types

5.5.4.1 CadServers

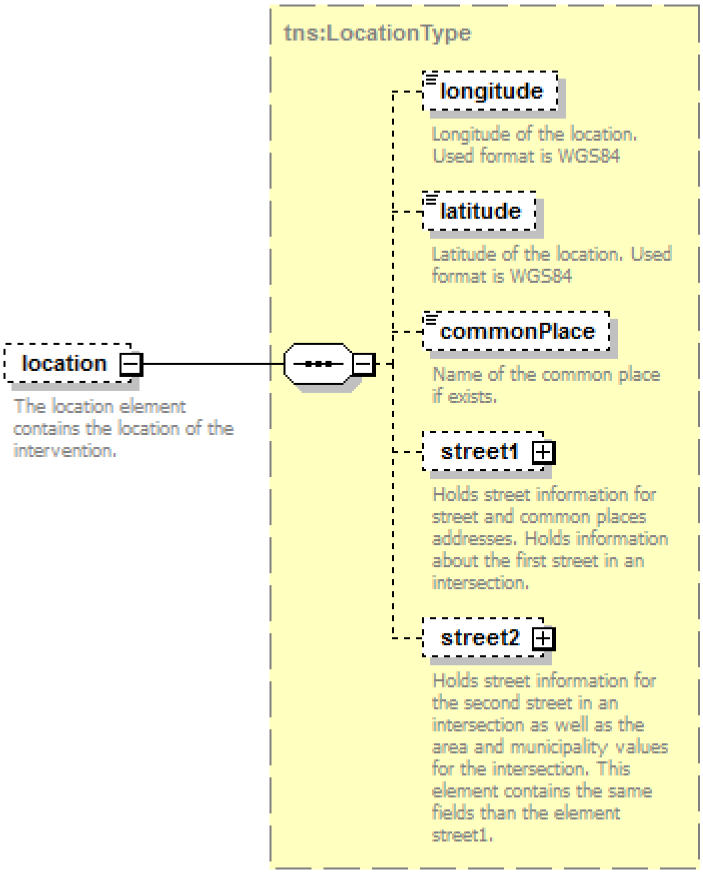
The CADServer element. It contains one or more server elements. The order in which the server elements are specified will be the order in which the SMUREG service contacts the CAD servers (phase 2).


tns:CadServersType
cadServers
The CADServer element. It contains one or more server elements. The order in which the server elements are specified will be the order in which the Smureg service contacts the CAD servers (phase 2).
server
The server element contains two sub elements for each CAD server.

Field name	Descriptions
server	The server element contains two sub elements for each CAD server.

5.5.4.2 Location

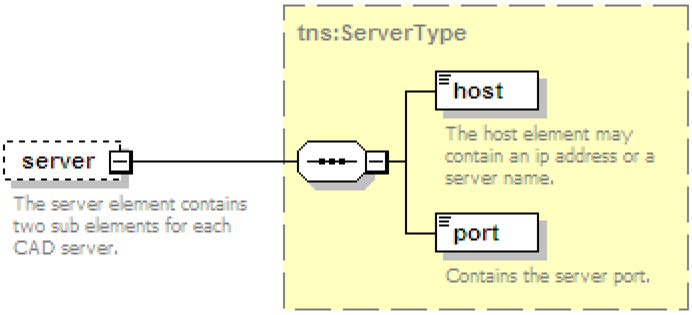
The location element contains the location of the intervention.


tns:LocationType
longitude
Longitude of the location. Used format is WGS84
latitude
Latitude of the location. Used format is WGS84
commonPlace
Name of the common place if exists.
street1
Holds street information for street and common places addresses. Holds information about the first street in an intersection.
street2
Holds street information for the second street in an intersection as well as the area and municipality values for the intersection. This element contains the same fields than the element street1.
location
The location element contains the location of the intervention.

Field name	Descriptions
longitude	Longitude of the location. Used format is WGS84
latitude	Latitude of the location. Used format is WGS84
commonplace	Name of the common place if exists.
street1	Holds street information for street and common places addresses. Holds information about the first street in an intersection.
street2	Holds street information for the second street in an intersection as well as the area and municipality values for the intersection. This element contains the same fields than the element street1.

5.5.4.3 Servers

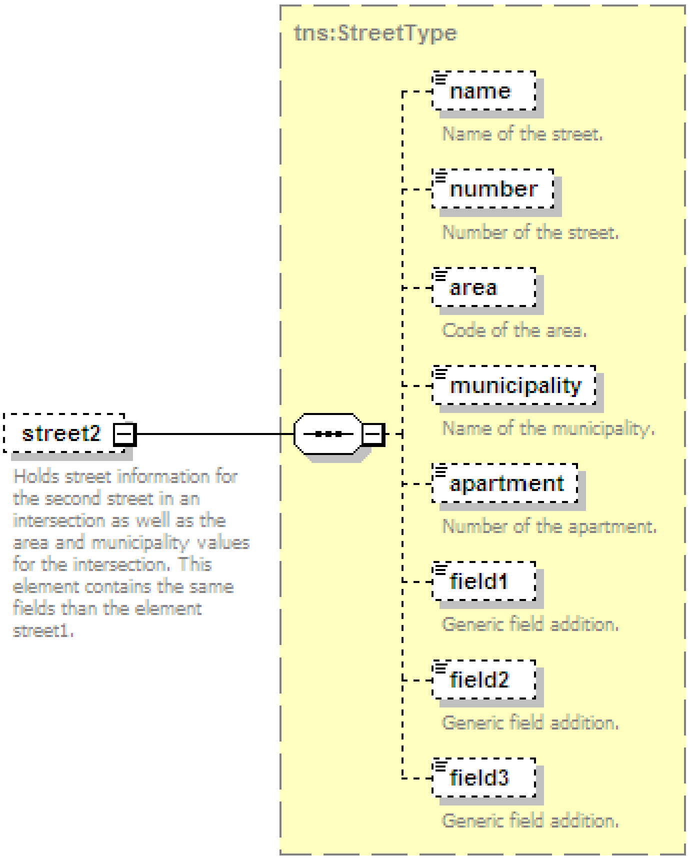
The server element contains two sub elements for each CAD server.


tns:ServerType
server
The server element contains two sub elements for each CAD server.
host
The host element may contain an ip address or a server name.
port
Contains the server port.

Field name	Descriptions
host	The host element may contain an IP address or a server name.
port	Contains the server port.

5.5.4.4 Street

Holds street information for street and common places addresses.



Field name	**Descriptions**
name	Name of the street.
number	Number of the street.
area	Code of the area.
municipality	Name of the municipality.
apartment	Number of the apartment.
field1	Generic field addition.
field2	Generic field addition.
Field3	Generic field addition.

6 Risks and security

6.1 Security

6.1.1 Business security

In case the development adds an additional use case based on an existing integration, eHealth 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 web service, the partner may obtain support from the contact center that is responsible for this service.

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

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

6.1.2 Web service

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

- SSL one way
- Time-to-live of the message: one minute.
- Signature of the timestamp, body and binary security token. This will allow eHealth 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 and are not allowed to transfer.
Every user takes care of his username, password and token and is forced to confidentiality of it. Every user is also responsible of every use which includes the use by a third party, until the inactivation.

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

For further information and instructions, please contact: info@ehealth.fgov.be.

7.1.4 Operational follow-up

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

7.2 Test cases

eHealth recommends performing tests for all of the following cases:

- Send an SDS message thanks to *SaveIntervention* and get a successful acknowledgement.
- Delete an intervention and get a successful acknowledgement.

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

- Send an SDS message with unexpected field values (values not know by the established mappings) and get a *validation error (100)* or *normalization error (200)*.
- Send an SDS message that was already sent and get an *SDS already exists (300)* error.
- Send a mal formed SDS message and get an *XSD compliance failure.*
- Delete an intervention with unexpected field values (values not know by the established mappings) and get a validation error (100) or normalization error (200).

  Delete two times the same intervention and get a validation error (100).

8 Error and failure messages

8.1 SaveIntervention Response Status Codes

Error codes originating from the eHealth platform:

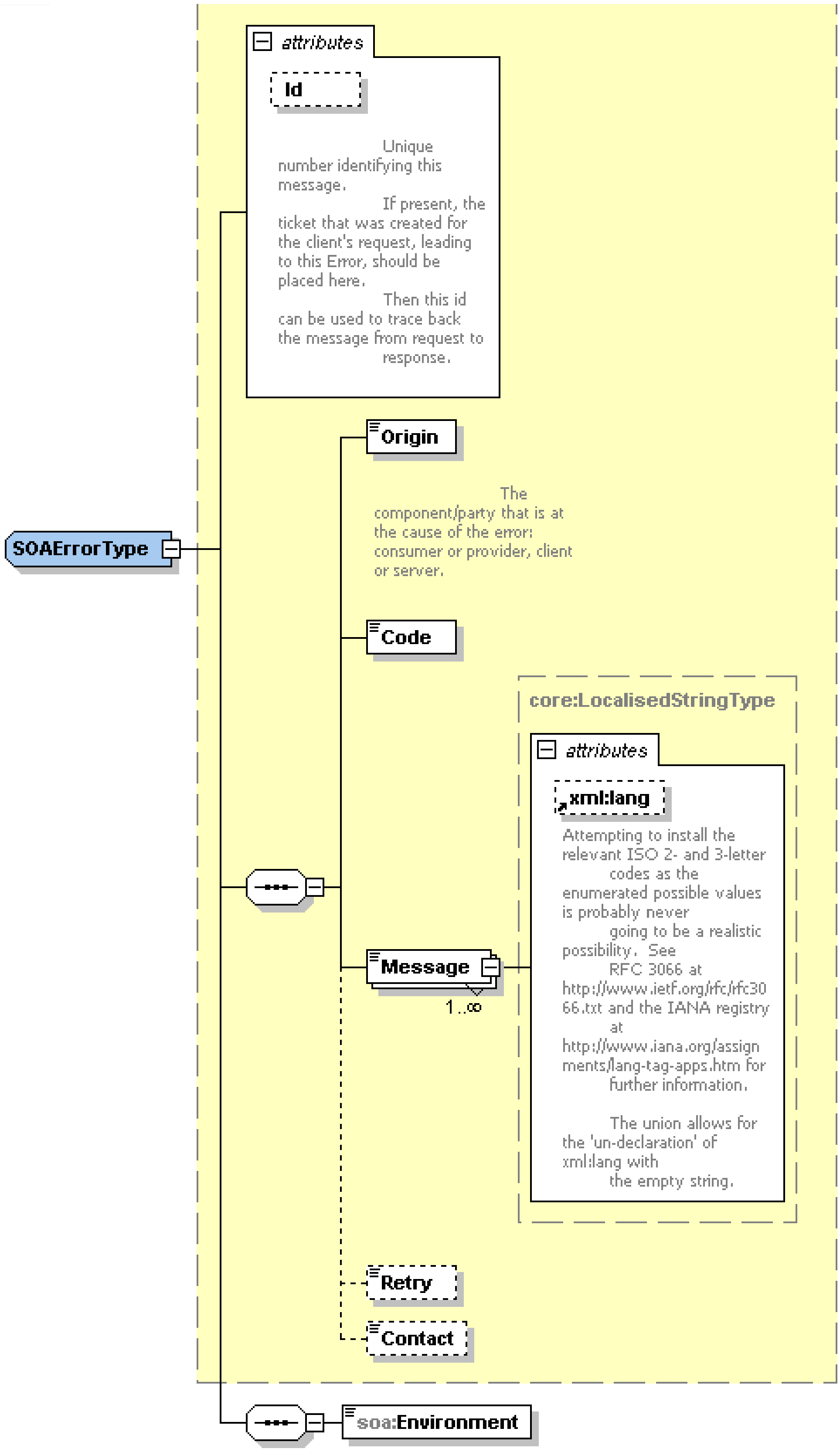
These error codes first indicate a problem in the arguments sent.

Code	Component	Description	Solution	Retry
100	SaveIntervention	Business validation errors.	Check the listed items. If necessary, contact the development team.	False
200	SaveIntervention	Received field values do not match the expected field values.	Check the field values causing problems. If necessary, contact the development team.	False
300	SaveIntervention	SDS Message already stored. Duplicate entry prevention.	You do not need to send this message again, it is already stored.	False

8.2 Soap Fault Error Codes

They contain the following attributes:

Field name	Descriptions
Id	Unique number identifying this message. If present, the ticket that was created for the client's request, leading to this error, should be placed here. Then this id can be used to trace back the message from request to
Origin	The component/party causing the error: consumer or provider, client or server.
Code	The Error Code
Message	A human readable message
Retry	An optional Boolean that indicates if it is worth resending the same Request.
Contact	An optional field specifying a contact description.
Environment	The environment in which the error occurs: development, test, integration, simulation, acceptation or production.


attributes
Id
Unique number identifying this message.
If present, the ticket that was created for the client's request, leading to this Error, should be placed here.
Then this id can be used to trace back the message from request to response.
SOAErrorType
Origin
The component/party that is at the cause of the error: consumer or provider, client or server.
Code
core:LocalisedStringType
attributes
xml:lang
Attempting to install the relevant ISO 2- and 3-letter codes as the enumerated possible values is probably never going to be a realistic possibility. See RFC 3066 at http://www.ietf.org/rfc/rfc3066.txt and the IANA registry at http://www.iana.org/assignments/lang-tag-apps.htm for further information.
The union allows for the 'un-declaration' of xml:lang with the empty string.
Message
1..∞
Retry
Contact
soa:Environment

8.2.1 Schema Validation Errors

When invoking the Web Service, a valid XML must be provided.

Before executing any action, the eHealthBox system verifies if the XML is valid by running a validation check towards the SendMessageRequest XSD.

If the validation fails, a SOAP Fault is returned with the following code and message:

Code	Message	Description	Solution	Retry
SOA-03001	Malformed message	This is the default error for content related errors in case no more details are known.	Consider all solutions below. If necessary, contact the development team.	False
SOA-03002	Message must be SOAP	Message does not respect the SOAP standard.	Check the sent SOAP request. If necessary, contact the development team.	False
SOA-03003	Message must contain SOAP body	Message respects the SOAP standard, but body is missing.	Check that the SOAP body element is present. If necessary, contact the development team.	False
SOA-03004	WS-I compliance failure	Message does not respect the WS-I standard.	Check the sent message. If necessary, contact the development team.	False
SOA-03005	WSDL compliance failure	Message is not compliant with WSDL.	Validate the message against WSDL & XSDL. If necessary, contact the development team.	False
SOA-03006	XSD compliance failure	Message is not compliant with XSD.	Validate the message against WSDL & XSDL. If necessary, contact the development team.	False
SOA-03007	Message content validation failure	From the message content (conform XSD): extended checks on the element format failed or cross-checks between fields failed.	Validate the message against WSDL & XSDL. If necessary, contact the development team.	False

Example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="id-6">
<soapenv:Fault>
<faultcode>soapenv:Client</faultcode>
<faultstring>SOA-03006</faultstring>
<detail>
<soa:SystemError xmlns:soa="urn:be:fgov:ehealth:errors:soa:v1" Id="5bbd8a2a-bb21-4cf8-99bc-8d52c18e2801">
<Origin>Consumer</Origin>
<Code>SOA-03006</Code>
<Message xml:lang="en">XSD compliance failure.</Message>
<soa:Environment>Production</soa:Environment>
```

```
</soa:SystemError>
</detail>
</soapenv:Fault>
</soapenv:Body>
</soapenv:Envelope>
```

8.2.2 Technical Errors

Technical errors are errors inherent to the internal working of the eHealth Web Service. It can also occur if the token used to call the web service is not valid.

They contain the standard SOAP Fault attributes.

The table provides de different code and message returned in a SOAP fault message:

Code	Message	Description	Solution	Retry
SOA-00001	An internal error has occurred. Please contact service desk.	This is the default error sent to the consumer in case no more details are known.	This can be a temporary error. If it persists, contact Supervision.	True
SOA-01001	Service call not authenticated.	From the security information provided, either the consumer could not be identified or the credentials provided are not correct.	This can be a temporary error. Request a new Token and retry. Could be a problem with the authentication. If persists contact Supervision Team.	True after requesting new token
SOA-01002	Service call not authorized.	The consumer is identified and authenticated, but is not allowed to call the given service.	Same as above.	True after requesting new token
SOA-02001	Service not available. Please contact service desk.	An unexpected error has occurred. Service desk may help with root cause analysis.	This can be a temporary error. If it persists, contact Supervision.	True
SOA-02002	Service temporarily not available. Please try later.	An unexpected error has occurred. Retries should work. If the problem persists service desk may help.	This can be a temporary error. If it persists, contact Supervision.	True

This list can evolve.

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<env:Body xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
<env:Fault>
<faultcode>soapenv:Server</faultcode>
<faultstring>SOA-00001</faultstring>
<detail>
```

```
<soa:SystemError Id="ec582704-d623-4b05-ab7f-98d5c9706dd1" xmlns:soa="urn:be:fgov:ehealth:errors:soa:v1">

<Origin>Server</Origin>

<Code>SOA-00001</Code>

<Message xml:lang="en">An internal error has occured. Please contact service desk.</Message>

<soa:Environment>Production</soa:Environment>

</soa:SystemError>

</detail>

</env:Fault>

</env:Body>

</soapenv:Envelope>
```

9 List of sources

This list is a summary of all links used in the document referring to internet resources. eHealth has no responsibility for these links.

	Date
http://www.w3.org/standards/xml/	24/03/11
http://www.oasis-open.org/specs/	24/03/11
http://www.w3.org/TR/soap12-mtom/	30/09/11

10 Annex 1 – Expected field values

The following mappings have been established between the different parties and are recognized by the SMUREG system.

Please use the expected values for each field in the tables below.

10.1 Expected values for “originator”

The field "originator" identifies the sender’s type. SMUREG determines if the request was issued by Intergraph or CityGIS based on this information.

SMUREG	Intergraph	CityGIS
N.A.	CIC	C100

10.2 Expected values for “eventNumber”

The field "eventNumber" uniquely identifies the intervention.

SMUREG	Intergraph	CityGIS
PPYYDDDZZZZ where - PP specifies the province of the 100 central: 10 = Antwerpen 20 = Brussels 21 = Leuven 22 = Wavre 30 = Brugge 40 = Gent 50 = Mons 60 = Liège 70 = Hasselt 80 = Arlon 90 = Namur - YY represents the last two digits of the year - DDD, the number of days in the year [1-366] - ZZZZ, the number of intervention in the day E.g. 40111650001	DSyydddnnnn where - D specifies the discipline (eg M = Medical) - S is the site: A (NT) = Antwerpen B (XL) = Brussels F (BRW) = Brabant G (LIE) = Liège H (AI) = Hainaut L (IM) = Limburg N (AM) = Namur O (V) = Oost Vlaanderen V (BR) = Vlaams-Brabant W (VL) = West-Vlaanderen X (LUX) Luxembourg = - yy represents the last two digits of the year - ddd, the number of days in the year [1-366] - nnnn, the number of intervention in the day E.g. MO111650001	Same as SMUREG

10.3 Expected values for “mobileRadio”

The identifier of the radio unit on the intervention.

SMUREG	Intergraph	CityGIS
A number that may not exceed 7 digits	Same as SMUREG	Currently CityGIS uses a symbol to identify the radios and will send a radio id.

10.4 Expected values for “typeOfCaller”

Identifies the type of the caller having dialed 100/112.

SMUREG	Intergraph	CityGIS
1 – Practitioner 2 – SMUR 3 – Ambulance 4 – Hospital 5 – Rest home 6 – Police 7 – Firemen 8 – Private 9 – Other 10 – Unknown 11 – PIT By default, 10 – Unknown.	10 – Unknown Currently not present in the Astrid CAD system.	Has its own table, but will map its values to the SMUREG list. If no value is specified, 10 - Unknown is sent. If a value is specified but no match exists, 9 - Other is sent.

10.5 Expected values for “interventionPlace”

Identifies the type of intervention place.

SMUREG	Intergraph	CityGIS
1 – Private 2 – Public 3 – Traffic 4 – School & Kindergarten 5 – Work 6 – Sport 7 – Other 8 – Secondary transfer 9 – Unknown 10 – MR/MRS 11 - Preventive	9 – Unknown Currently not present in the Astrid CAD system.	9 – Unknown

10.6 Expected values for “transportCode”

SMUREG	Intergraph	CityGIS
1 – requested by: patient/family 2 – requested by: 100 3 – requested by: controller/regulator 4 – requested by: general practitioner	8 – Code K – Nutteloze Oproep 10 - Code T – Transport door derde 16 - Code Z – Geen slachtoffers 17 - Code D – Patiënt Overleden By default: null.	Will map their own codes to those of SMUREG

5 – requested by: SMUR doctor 6 – no transport: deceased after CPR 7 – no transport: deceased without CPR 8 – no transport: useless 9 – no transport: fake call 10 – no transport: already taken in charged/gone 11 – no transport: refusal 12 – no transport: cancelled 13 – no transport: unknown 14 – requested by: other 15 – requested by: unknown 16 – no transport: no patient 17 – no transport: death diagnosis		

10.7 Expected values for “hospitalCode”

This will be the hospital code. SMUREG will not be able to convert hospital names to know hospital codes.

SMUREG	**Intergraph**	**CityGIS**
Hospital codes	Intergraph will send the hospital name and no hospital code will be sent. No information will be stored for this value in the SMUREG Database.	Will map the hospital to the corresponding SMUREG hospital code.