TimeStamping Consult v2.0
Cookbook
Version 1.5

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

eHealth platform

Willebroekkaai 38 – 1000 Brussel
38, Quai de Willebroeck – 1000 Bruxelles

Table of contents

To the attention of: "IT expert" willing to integrate this web service.

1. Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1.0	13.10.2014	eHealth platform	Initial version
1.1	27.10.2016	eHealth platform	Updated endpoint for TSC V1
1.2	05.07.2017	eHealth platform	p.m.
1.3	01/06/2018	eHealth platform	Update
1.4	24/04/2021	eHealth platform	WS-I Compliance Tracing
1.5	11/07/2022	eHealth platform	§ 2.3 eHealth platform document references (updated) § 3.2 Status (added) § 5.1.3 Tracing (updated)

2. Introduction

Within the Belgian hospitals more ICT systems are being introduced to support the daily operations. Consequently, the hospitals are migrating towards a paperless environment where information is electronically stored.

This makes it more difficult for the supervising authorities to fulfil their duties, as today the paper documents are the most important source of proof of activities. However, migrating to an environment where all information is kept in an ICT environment also introduces new opportunities as the timestamp service.

2.1 Goal of the service

This document provides technical information on calling the web service(WS) Timestamping Consult of the eHealth platform. The goal of this service is to offer a possibility for consulting the archive fed by the timestamp authority service. This service allows you to check two things:

- The existence of a certain document at the moment it was timestamped.

- The completeness of a list of timestamped documents during a certain period of time.

If you want to use this service, it is therefore necessary that you also use the timestamp authority service (see Cookbook Timestamping Authority).

As it exists two versions of the service TSA, it exists two versions of the service TSC. TSC V1 is compatible with TSA V1 and TSC V2 is compatible with TSA V2.

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.

However, in order to interact in a smooth, homogeneous and risk controlled way with as many partners as possible, 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 Support section 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			eHealth platform
2	Timestamping Authority - Cookbook	1.6	11/07/2022	eHealth platform

---

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

2.4 External document

All documents can be found through the internet. They are available to the public, but not supported by eHealth.

ID	Title	Source	Date	Author
1	RFC3161	*http://www.ietf.org/rfc/rfc3161.txt*	22/09/2010	Network Working Group
2	XML Timestamping Profile of the OASIS Digital Signature Services	*http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-timestamping-spec-v1.0-os.pdf*	22/09/2010	OASIS
3	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

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.

4. Global overview

4.1 Web services

The timestamping project is composed by two web services:

4.1.1 Timestamp Authority (TSA)

This service contains one operation called **SignRequest,** which performs the classical operations of a timestamping authority on a document:
There are two possible ways to send documents to the timestamp server, either as a simple document or as a hash code. In both cases, the client must send the value in Base64. The server checks if it has received a hash code. If not, it calculates the hash code of the document received. Next, it concatenates a timestamp to the hash of the document and it calculate the hash of this result. Then this hash is digitally signed with the private key of eHealth and a timestamp token is created and returned to the user. The timestamp token contains the information the client application will need to verify the timestamp later. The timestamp authority service implements the OASIS-DSS protocol but does not support multiple documents request. The response token is defined by the RFC 3161 protocol.

Moreover, this service offers the possibility to store the received document in the eHealth archive in order to verify the integrity of the user's archive later. By default, the archiving is only activated for the hospitals of the project Electronic Prescription in Hospitals. For the other projects, the archiving is not activated so the user has to make a special requirement to **_support@ehealth.fgov.be_** if he wants to activate it (see more information in point 5.3.1.1).

4.1.2 Timestamp Consult (TSC)

As its name suggests, this service allows to consult the archive of the time stamp server (for more details, see the cookbook Timestamp Consult service). It contains two operations:

- **TSConsultTSBagRequest**: Consultation by sending a sequence number and a time (in milliseconds expressed as UTC time). The server will respond with the corresponding timestamp.
- **TSConsultRequest**: Consultation by sending a period and a list of sequences numbers and times. The server will respond with a list of missing timestamps. It offers the client the possibility to check if his own archive is complete.

Naturally, if the archiving is not configured for a user, he cannot use the service of consultation.

4.1.3 Electronic Prescription in Hospitals

Within the framework of the electronic prescription in hospitals, the use of the timestamping services is governed by a legal context.
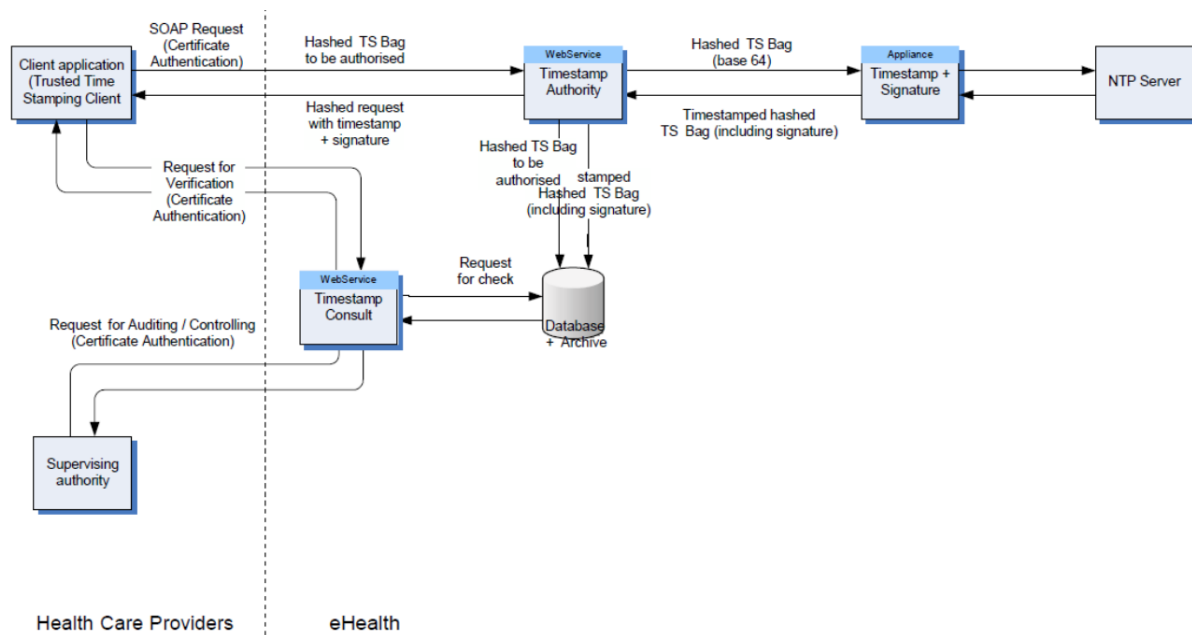
The hospital doctor issues an electronic prescription (the document to be timestamped) which is hashed. Every five minutes, the hashed prescriptions are collected in a package called "TimeStampBag". This bag is sent to the eHealth Platform through the web service *Timestamp Authority* so that it can be timestamped. The timestamp token generated from the bag is sent to the hospital for preservation in its archive. On the eHealth Platform side, a copy of the bag and its timestamp is also stored in the archives.

When the hospital wishes, it can consult the eHealth archives through the web service Timestamp Consult in order to compare their content and the content of the archives of the hospital. All the bags contained in the archives of the hospital should normally be stored in the eHealth archives. Naturally, a hospital can consult only its own bags in the eHealth archives; it cannot consult the bags of another hospital.

Moreover, the NIHDI can also consult the archives of the eHealth Platform (linked to any hospital) through the web service Timestamp Consult for auditing and controlling as a supervising authority.

5. Step-by-step

5.1 Technical requirements

The client must have a certificate to use the service (see paragraph 3.4).

Next he must use the eHealth Timestamp Authority service before using the eHealth Timestamp Consult service.

5.1.1 Security policies to apply

You must use SSL one way for the transport layer.

As WS 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, it will not be treated).

- The signature with the certificate of

  o the timestamp, (the one mentioned above),

  o the body (the message itself),

  o and the binary security token: an eHealth certificate.

  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 by eHealth.

5.1.2 WS-I Basic Profile 1.1

Your request must be WS-I compliant (See Chap 2 - External Ref). If not you will receive one of the errors SOA-03001 – SOA-03003 5See Chap 8 – Errors and failures).

5.1.3 Tracing

5.1.4 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   Process overview

The partner who wishes to use the timestamping service(s) must first contact eHealth (***info@ehealth.fgov.be***) in order to specify clearly the context and the purpose of his project. If his request is validated, he must obtain a certificate (see paragraph 3.4) and contact eHealth to configure his profile. Then, everything is ready to start using the service.

NB: Within the framework of the electronic prescription in hospitals, the hospital must fill and sign the protocol found here ***https://www.ehealth.fgov.be/ehealthplatform/fr/service-datation-electronique-timestamping***.

5.3   Web service

The WS TSA V2 contains one operation called "SignRequest" and it has the following endpoints:

- Integration environment: ***https://services-int.ehealth.fgov.be/TimestampConsult/v2***

- Acceptance environment: ***https://services-acpt.ehealth.fgov.be/TimestampConsult/v2***

- Production environment: ***https://services.ehealth.fgov.be/TimestampConsult/v2***

Note: When not described, fields may be ignored.

For information, here are the endpoints of TSC V1 (if you used previously the service TSA V1):

- Integration environment: ***https://services-int.ehealth.fgov.be/TimestampConsult/v1***

- Acceptance environment: ***https://services-acpt.ehealth.fgov.be/TimestampConsult/v1***

- Production environment: ***https://services.ehealth.fgov.be/TimestampConsult/v1***

5.3.1   TSConsultTSBagRequest

Get the timestamp corresponding to a sequence number and the time.

5.3.1.1   Input arguments
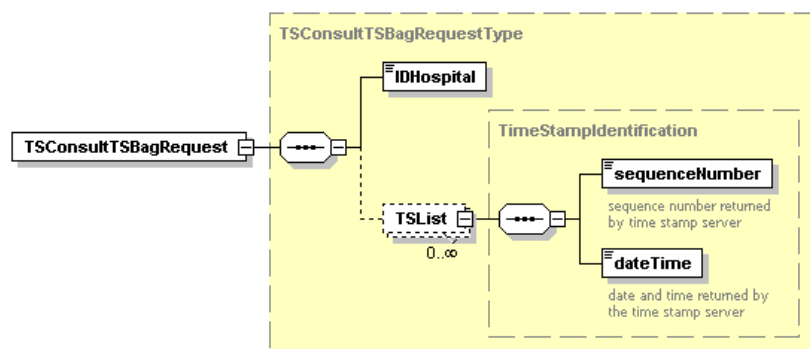
Field name	Description
IDHospital	Unique Identifier of the client
sequenceNumber	Sequence number returned by the timestamp authority service
dateTime	Time returned by the timestamp authority service

5.3.1.2 Output arguments
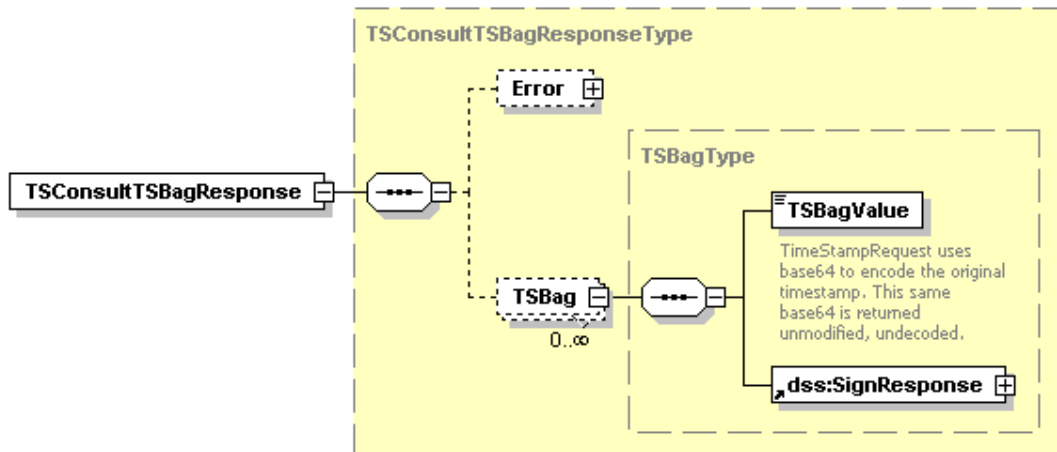
Field name	Description
TSBagValue	Timestamp corresponding to the sequence number of the request

5.3.1.4 Example

Request:

```
<urn:TSConsultTSBagRequest>
  <urn:IDHospital>tsa_0406798006_01</urn:IDHospital>
  <urn:TSList>
    <urn:sequenceNumber>1234782014279</urn:sequenceNumber>
    <urn:dateTime>1234782014000</urn:dateTime>
  </urn:TSList>
</urn:TSConsultTSBagRequest>
```

Reply:

```
<ns2:TSConsultTSBagResponse xmlns="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns2="urn:be:fgov:ehealth:timestamping:protocol:v2"
xmlns:ns3="urn:oasis:names:tc:dss:1.0:core:schema" xmlns:ns4="urn:oasis:names:tc:SAML:1.0:assertion">
  <ns2:TSBag>
    <ns2:TSBagValue>Supervission</ns2:TSBagValue>
    <ns3:SignResponse Profile="urn:ehealth:profiles:timestamping:1.0">
      <ns3:Result>
        <ns3:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</ns3:ResultMajor>
        <ns3:ResultMinor>urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:OnAllDocuments
        </ns3:ResultMinor>
      </ns3:Result>
      <ns3:SignatureObject>
        <ns3:Timestamp>
          <ns3:RFC3161TimeStampToken>
```

MIICaDAVAgEAMBAMDk9wZXJhdGlvbiBPa2F5MIICTQYJKoZIhvcNAQcCoIICPjCCAjoCAQMxDzANBglghkgBZQME
AgEFADBlBgsqhkiG9w0BCRABBKBWBFQwUgIBAQYBKjAxMA0GCWCGSAFlAwQCAQUABCBAzVdYEqrZpHS7GEdJ
AFX3Kg0CJmB33ysP8Guolo8VEAIGAR9+vktHGA8yMDA5MDIxNjExMDAxNFoxggG7MIIBtwIBATB2MGwxCzAJBg
NVBAYTAkJFMREwDwYDVQQIEwhCcnVzc2VsczERMA8GA1UEBxMIQnJ1c3NlbHMxDjAMBgNVBAoTBVNtYWwzM
RAwDgYDVQQLEwdISGVhbHRoMRUwEwYDVQQDEwxlSGVhbHRoIFRlc3QCBgEZn9zayzANBglghkgBZQMEAgEFA
KCBmDAaBgkqhkiG9w0BCQMxDQYLKoZIhvcNAQkQAQQwHAYJKoZIhvcNAQkFMQ8XDTA5MDIxNjExMDAxNFow
KwYLKoZIhvcNAQkQAgwxHDAaMBgwFgQUCA3Z8J2qHlCl3Vq5ASl5MdEjV/swLwYJKoZIhvcNAQkEMSIEIMPzVfnd
Eg6z3zYFyVx9uHhu8kbAvrMZpMIIDokDL8CsMA0GCSqGSIb3DQEBAQUABIGAPOLQu6DPruu8Z1Q6OI5Tp5WFkaJ
QrDVrshpQnEiKyKOJ9vtv2C6aO3VvNAZG/5YMHeeTFQrscM76s/ZKWfrRGTVNFu1e0q9dg8BAw7g1XG5oAmyK42
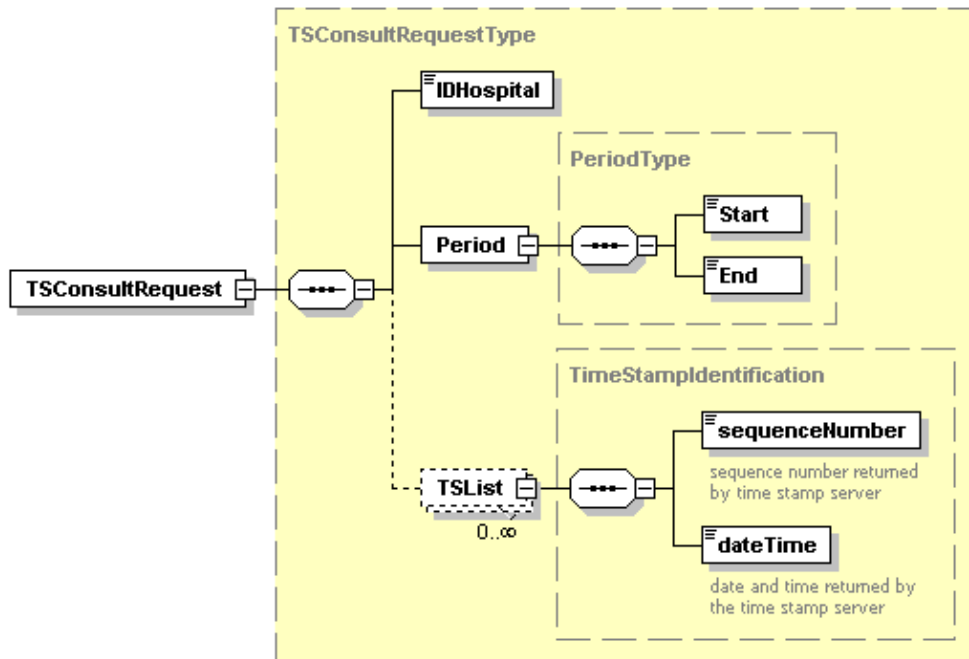5jOvMAHLukbzrUMW98d29n87q4rEpB7yx/qOWbaTwDNtX+d+g4kPiyO7A=</ns3:RFC3161TimeStampToken>

```
        </ns3:Timestamp>
      </ns3:SignatureObject>
    </ns3:SignResponse>
  </ns2:TSBag>
</ns2:TSConsultTSBagResponse>
TSConsultRequest
```
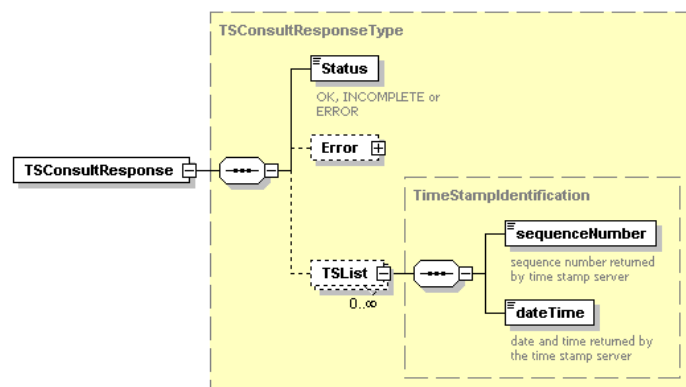
Check the completeness of the list of timestamps.

5.3.1.5 Input arguments

Field name	Description
IDHospital	Unique Identifier of the client
sequenceNumber	Sequence number returned by the timestamp authority service
dateTime	Time returned by the timestamp authority service
Start	Start time of the period
End	End time of the period

5.3.1.6 Output arguments

Field name	Description
Status	Status of the list (OK, INCOMPLETE, ERROR)
sequenceNumber	Sequence number returned by the timestamp authority service
dateTime	Time returned by the timestamp authority service

5.3.1.7 Example

Request:

```xml
<urn:TSConsultRequest>
    <urn:IDHospital>tsa_0406798006_01</urn:IDHospital>
    <urn:Period>
      <urn:Start>1234782013999</urn:Start>
      <urn:End>1234782014001</urn:End>
    </urn:Period>
    <urn:TSList>
      <urn:sequenceNumber>1234782014279</urn:sequenceNumber>
      <urn:dateTime>1234782014000</urn:dateTime>
    </urn:TSList>
</urn:TSConsultRequest>
```

Reply:

```xml
    <ns2:TSConsultResponse xmlns="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns2="urn:be:fgov:ehealth:timestamping:protocol:v2"
xmlns:ns3="urn:oasis:names:tc:dss:1.0:core:schema" xmlns:ns4="urn:oasis:names:tc:SAML:1.0:assertion">
    <ns2:Status>OK</ns2:Status>
    </ns2:TSConsultResponse>
```

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, the eHealth platform must be informed at least one month in advance with a detailed estimate of the expected load. This will ensure an effective capacity management.

In case of technical issues on the WS, the partner may obtain support from the contact center (see Chap 3)

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

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

6.1.2 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 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 must not be shared. Every user is responsible for his username, password, and token and must ensure their confidentiality. Every user is also responsible for every use including the use by a third party, until inactivation.

7. Test and release procedure

7.1 Procedure

This chapter explains the procedures for testing and releasing an application in acceptance 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 WS. Most of the required integration information is published on the Support section of 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 access to the eHealth acceptance environment.

From this moment, you start integration and acceptance tests. The eHealth platform suggests performing tests during at least one month.

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

Then the eHealth platform and the partner agree on a release date. The eHealth platform prepares the connection to the production environment and provides the partner with the necessary information. During the release day, the partner provides 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 his applications will always test first in the acceptance environment before releasing any adaptations of his application in production. In addition, he will inform eHealth on the progress and test period.

8. Error and failure messages

8.1 Error codes originating from the eHealth platform:

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

Error code	Description
OASIS_RESULT_MAJOR_REQUESTER_ERROR	The request is invalid
OASIS_RESULT_MAJOR_RESPONDER_ERROR	An error occurred on the server side

When an error occurred, a detailed message is sent.

8.2 WS-I Basic Profile 1.1 - Errors

SOA-03001	*Malformed message*	*Consumer*	*This is the default error for content related errors in case no more details are known.*
SOA-03002	*Message must be SOAP*	*Consumer*	*Message does not respect the SOAP standard.*
SOA-03003	*Message must contain SOAP body*	*Consumer*	*Message respects the SOAP standard, but body is missing.*