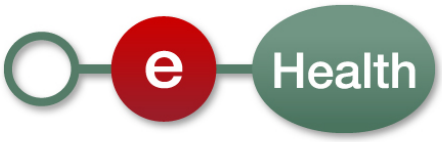


Cookbook
Belgian Resident Assessment Instrument (BelRAI)
web service

This document is provided to you free of charge by the

eHealth platform

Willebroekkaai 38

38, Quai de Willebroek

1000 BRUSSELS

Table of contents

1. Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1	05/05/2015	eHealth	Document creation

2. Introduction

2.1 Goal of the service

BelRAI (Belgian Resident Assessment Instrument) web services enable the exchange of BelRAI assessment data between software systems and the central BelRAI database.

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			eHealth
2	eHealth STS	1.1	31/08/2010	eHealth
3	Cookbook "bekende bestemmeling/destinataire connu"	2.3	06/05/2011	eHealth

2.4 External document references

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	OASIS SAML Token Profile	***http://www.oasis-open.org/committees/download.php/16768/wssv1.1-spec-os-SAMLTokenProfile.pdf***	01/02/2006	OASIS
2	BelRAI cookbook	**http://www.belrai.org/BelRAI_Cookbook_webservices.docx**	N.A	BelRAI

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

3. Business and privacy requirements

3.1 Certificates

An eHealth certificate is used to identify the initiator of the request. If you don't have one, see:

Dutch version:
https://www.ehealth.fgov.be/nl/support/basisdiensten/ehealth-certificaten

French version:

https://www.ehealth.fgov.be/fr/support/services-de-base/certificats-ehealth

For technical issues regarding eHealth certificates

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

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

3.2 BelRAI contact

For questions about the business content of the message, please contact the BelRAI helpdesk:

E-mail : helpdesk@belrai.org

Tel. 013/22.90.34

3.3 Support in general

For issues in production only

eHealth ContactCenter:

- Phone: 02/788 51 55
- Mail: ***support@ehealth.fgov.be***
- *Contact Form :*

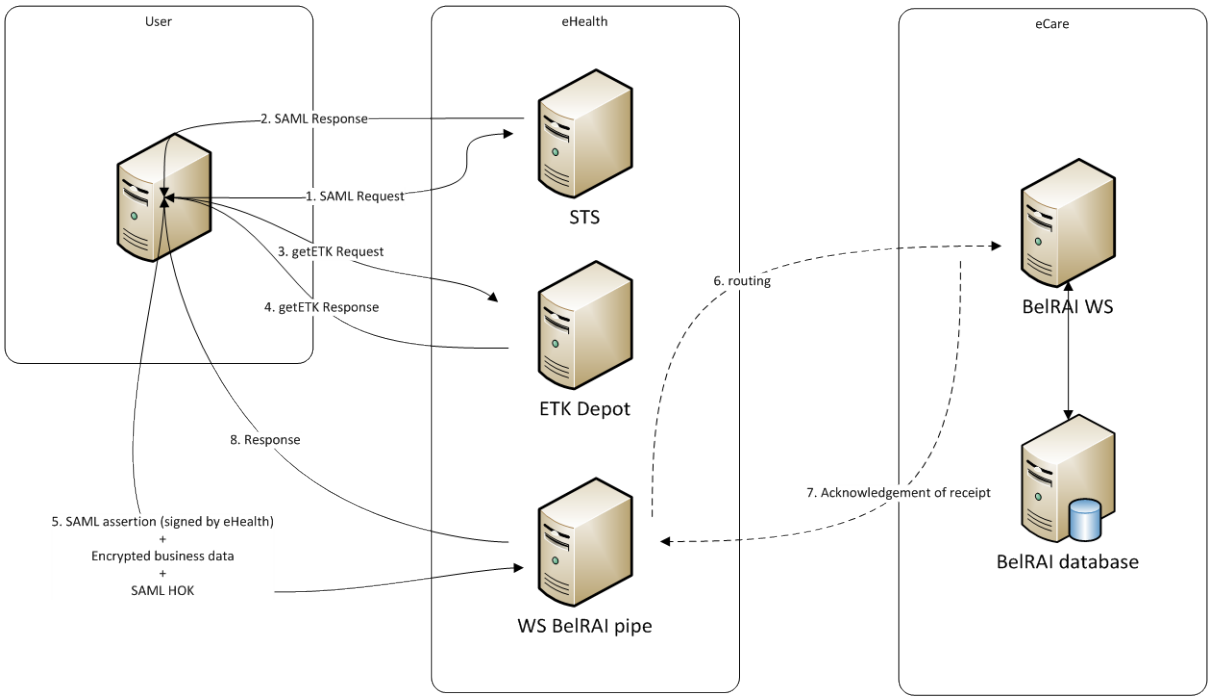
https://www.ehealth.fgov.be/nl/neem-contact-met-de-openbare-instelling-eHealth-platform (Dutch)

https://www.ehealth.fgov.be/fr/contactez-institution-publique-plate-forme-eHealth (French)

FOR PARTNERS AND SOFTWARE DEVELOPERS ONLY

- For business issues please contact: ***info@ehealth.fgov.be***
- For technical issues in production please contact: ***support@ehealth.fgov.be or call 02/788 51 55***
- For technical issues in acceptance please contact: ***Integration-support@ehealth.fgov.be***

4. Global overview



The first step is to request a SAML token from our STS Service. See section 5.1.1 for more details. After receiving a valid token, an ETK is needed for the encryption of folder element of KHMER message. This ETK is retrieved from our ETK depot. See section 5.1.2 for more details.

The next step is to create the business message, encrypt it using the ETK and calling the WS BelRAI pipe.

5. Step-by-step

5.1 Technical requirements

5.1.1 Use of the eHealth SSO solution

The complete overview of the profile and a step-by-step implementation to start protecting a new application with SSO @ eHealth is described in the eHealth STS cookbook. In order to implement a call to the eHealth STS you can reuse the implementation as provided in the "eHealth technical connector":

- ***https://www.ehealth.fgov.be/fr/support/connectors***
- ***https://www.ehealth.fgov.be/nl/support/connectors***

Nevertheless, eHealth implementations use standards and any other compatible technology (web service stack for the client implementation) can be used instead. The attributes that need to be provided and the attributes that should be certified by eHealth in order to obtain a token valid for BelRAI services are described in sections 5.1.1.1 and 5.1.1.2. To access the BelRAI web services, the response token must contain “true” for all of the Boolean certification attributes and a value for all the nihii11 certification attributes. If you obtain “false” for one Boolean certification attributes or no value for the nihii11 certification attribute, please contact eHealth to verify that the requested test cases were correctly configured.

5.1.1.1 Hospital

The needed identification attributes are the following:

The NIHII number as identifier of the hospital
(namespace: “urn:be:fgov:identification-namespace”)
“urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number” and
“urn:be:fgov:ehealth:1.0:hospital:nihii-number”

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

The NIHII number as identifier of the hospital
(namespace: “urn:be:fgov:identification-namespace”)
“urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number” and
“urn:be:fgov:ehealth:1.0:hospital:nihii-number”

Attribute to verify if it is a recognized hospital
(namespace: "urn:be:fgov:certified-namespace:ehealth")
“urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number:recognisedhospital:boolean”

Attribute to get the nihii11 of a recognized hospital
(namespace: "urn:be:fgov:certified-namespace:ehealth")
“urn:be:fgov:ehealth:1.0:hospital:nihii-number:recognisedhospital:nihii11”

The documents REGISTER_STS_Hospital_samlRequest.xml and REGISTER_STS_Hospital_samlResponse.xml provide STS request/response examples for a hospital which has **access** to BelRAI web service.

The documents REGISTER_STS_Hospital_NoAccess_samlRequest.xml and REGISTER_STS_Hospital_NoAccess_samlResponse.xml provide STS request/response examples for a hospital which has **no access** to BelRAI web service.

You can find these examples in the archive BelRAI_STS_example.zip

5.1.1.2 Retirement

The needed identification attributes are the following:

> **The NIHII number as identifier of the retirement**
> (namespace: “urn:be:fgov:identification-namespace”)
> “urn:be:fgov:ehealth:1.0:certificateholder: retirement:nihii-number” and
> “urn:be:fgov:ehealth:1.0: retirement:nihii-number”

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

> **The NIHII number as identifier of the retirement**
> (namespace: “urn:be:fgov:identification-namespace”)
> “urn:be:fgov:ehealth:1.0:certificateholder:retirement” and
> “urn:be:fgov:ehealth:1.0:retirement:nihii-number”
>
> **Attribute to verify if it is a recognized retirement**
> (namespace: "urn:be:fgov:certified-namespace:ehealth")
> “urn:be:fgov:ehealth:1.0:certificateholder:retirement:nihii-number:recognisedretirement:boolean”
>
> **Attribute to get the nihii11 of a recognized retirement**
> (namespace: "urn:be:fgov:certified-namespace:ehealth")
> “urn:be:fgov:ehealth:1.0:retirement:nihii-number:recognisedretirement:nihii11”

The documents REGISTER_STS_Retirement_samlRequest.xml and REGISTER_STS_ Retirement _samlResponse.xml provide STS request/response examples for a retirement which has **access** to BelRAI web service.

The documents REGISTER_STS_ Retirement _NoAccess_samlRequest.xml and REGISTER_STS_ Retirement _NoAccess_samlResponse.xml provide STS request/response examples for a retirement which has **no access** to BelRAI web service.

You can find these examples in the archive BelRAI_STS_example.zip

5.1.2 Encryption

The folder element of KMEHR message to send to the web service must be encrypted.

To encrypt the message, you should retrieve the public key on the ETK (eHealth Token Key) depot. And then, encrypt the message using this public key via eHealth encryption libraries.

All the information about the use of the encryption libraries and the call to the ETK depot are described in the cookbooks available on the eHealth technical library on the eHealth website (“Cookbook bekende bestemmeling”/”Cookbook destinataire connu”). The table below provides you the identifiers to use in the GetEtkRequest.

Environment	Type	Value	Application ID
Acceptance Environment	CBE	0367303762	BELRAIFE
Production Environment	CBE	0367303762	BELRAIFE

More information can be found in the cookbook documents provided by BelRAI (see link in section 2.4).

5.1.3 Security policies to apply

We expect that you use SSL one way for the transport layer.

As web service security policy, we expect:

- A timestamp (the date of the request), with a Time to live of one minute (if the message doesn't arrive during this minute, it shall not be treated).
- The signature with the certificate of
  - the timestamp, (the one mentioned above)
  - the body (the message itself)
  - and the binary security token: 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 by eHealth.

The STS cookbook can be found on the eHealth portal, Technical Library.

5.2 Process overview

Summary:

To call the BelRAI web service:

- Add the encrypted folder element of KHMER message. See section 5.1.2.
- 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).
  - **Timestamp**.
  - A **signature** that has been placed on the SOAPBody 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.
  - KeyInfo with a SecurityTokenReference pointing to the SAML Assertion.

See also the WSSP in the WSDL[2].

As for now, only the operations described below are available. The operations for the web services are:

Operation	Description
PutTransactionRequest	Send assessment data to BelRAI. This can be a full assessment or only parts of it.
GetTransactionListRequest	Get list of assessments for a patient from BelRAI.
GetTransationRequest	Retrieve assessment data for a patient from BelRAI.
PutPatientRequest	Update/create patient profile in BelRAI.
GetPatientRequest	Retrieve patient profile from BelRAI.

[2] WSDL's can be found in the eHealth Service Registry:
https://services.ehealth.fgov.be/registry/uddi/bsc/web or ***https://services-acpt.ehealth.fgov.be/registry/uddi/bsc/web*** for services in the acceptance environment.

PutHCPartyRequest	Update/create caregiver profile in BelRAI.
GetHCPartyRequest	Retrieve caregiver profile from BelRAI.
PutPatientConsentRequest	Record in BelRAI that the BelRAI informed consent has been signed by this patient.
GetPatientConsentRequest	Retrieve from BelRAI if the BelRAI informed consent has been signed by this patient or not.
RevokePatientConsentRequest	Record in BelRAI that the BelRAI informed consent has been revoked by this patient.
GetTherapeuticLinkRequest	Retrieve the therapeutic relation status between caregiver and patient in BelRAI.
PutTherapeuticLinkRequest	Record in BelRAI the therapeutic relation status between caregiver and patient in BelRAI.

The endpoints and service contract (eHealth XSDs) for each of these operations can be found in the Registry on the eHealth portal, section 'Support - Tools'.

For more details about operations, see the cookbook documents provided by BelRAI (see link in section 2.4)

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.

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 (only the business part is encrypted).

7. Test procedure

This chapter explains the procedures for testing BelRAI WS in acceptance or production environment.

7.1 Request a test case

In order to be authorized to call the web services, the hospital must be configured in the eHealth acceptance environment. So, create an excel file like the below example and send it to ***info@ehealth.fgov.be*** with the subject: “BelRAI request test case”.

Identifier	**Name**	**Type**
Hospital or retirement identifier	Hospital or retirement name	Hospital or retirement

Example: hospital

Identifier	**Name**	**Type (hospital or retirement)**
99999971	Hospital test acc	Hospital

After the configuration is done, a certificate should be requested for hospital or retirement home.

7.2 Request a hospital or retirement certificate

The developed functionality needs to be tested using an acceptance certificate for hospital or retirement. Therefore a participating test-hospital or test-retirement must first have a certificate-responsible. Acceptance tests need to be performed on-site (in a pilot hospital or in a pilot retirement). Therefore, the hospital-acceptance or retirement-acceptance certificate is required. Software companies may only conduct acceptance tests in the acceptance environment of the hospital where the acceptance certificate and key pair of the specific environment shall be consulted on the predefined path (“Home Directory” under: \ehealth\keystore\ as set out in eHealth Certifcate Manager – manual section 2.1.12).

8. Error and failure messages

There are different possible types of response:

- If there are no technical errors, responses as described in section 5.3 are returned.
- In the case of a technical error, a SOAP fault exception is returned (see table below)

If an error occurs, first please verify your request. Following table contains a list of common system error codes for the eHealth Service Bus.

Description of the possible SOAP fault exceptions.

Error code	Component	Description	Solution/Explanation
SOA-00001	Unknown	Service error	This is the default error sent to the consumer in case no more details are known.
SOA-01001	Consumer	Service call not authenticated	From the security information provided, • or the consumer could not be identified • or the credentials provided are not correct
SOA-01002	Consumer	Service call not authorized	• The consumer is identified and authenticated, but is not allowed to call the given service.
SOA-02001	Provider	Service not available. Please contact service desk	• An unexpected error has occurred • Retries will not work • Service desk may help with root cause analysis
SOA-02002	Provider	Service temporarily not available. Please try later	• An unexpected error has occurred • Retries should work • If the problem persists service desk may help
SOA-03001	Consumer	Malformed message	This is a default error for content related errors in case no more details are known.
SOA-03002	Consumer	Message must be SOAP	Message does not respect the SOAP standard
SOA-03003	Consumer	Message must contain SOAP body	Message respects the SOAP standard, but body is missing
SOA-03004	Consumer	WS-I compliance failure	Message does not respect the WS-I standard
SOA-03005	Consumer	WSDL compliance failure	Message is not compliant with WSDL in Registry/Repository
SOA-03006	Consumer	XSD compliance failure	Message is not compliant with XSD in Registry/Repository
SOA-03007	Consumer	Message content validation failure	From the message content (conform XSD): • Extended checks on the element format failed • Cross-checks between fields failed