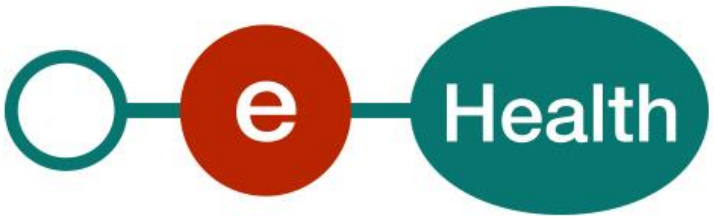


Identity & Authorization Management (I.AM)
SSO from fat to thin client
Technical specifications
Version 1.2

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	30/04/2015	eHealth platform	Initial version
1.1	30/10/2018	eHealth platform	Update linked to major release R2018.2
1.2	06/04/2022	eHealth platform	Review IDP screens (new look and feel)

2. Introduction

2.1 Context

A user (physical person), in possession of a sessionToken he received from the eHealth SecureTokenService (STS), needs to continue his work in a remote web application for which authentication at the eHealth platform is required. Therefore, he needs to identify himself at the eHealth IdentityProvider (IDP). As the user is already in possession of a sessionToken from the STS, he can reuse it to authenticate at the IDP.

2.2 Goal of the document

This document describes in detail how to use a secure token, delivered by the STS, as identity proof to start a web browser Single Sign on Session.

It does not contain details on how to get a secure token from the STS in the first place. Therefore, see the cookbook STS, available on the portal of the eHealth platform.
(***https://www.ehealth.fgov.be/ehealthplatform/nl/service-iam-identity-access-management***)

Important note : this approach is not available for secure token delivered by STS with eHealth institution/organization certificates.

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

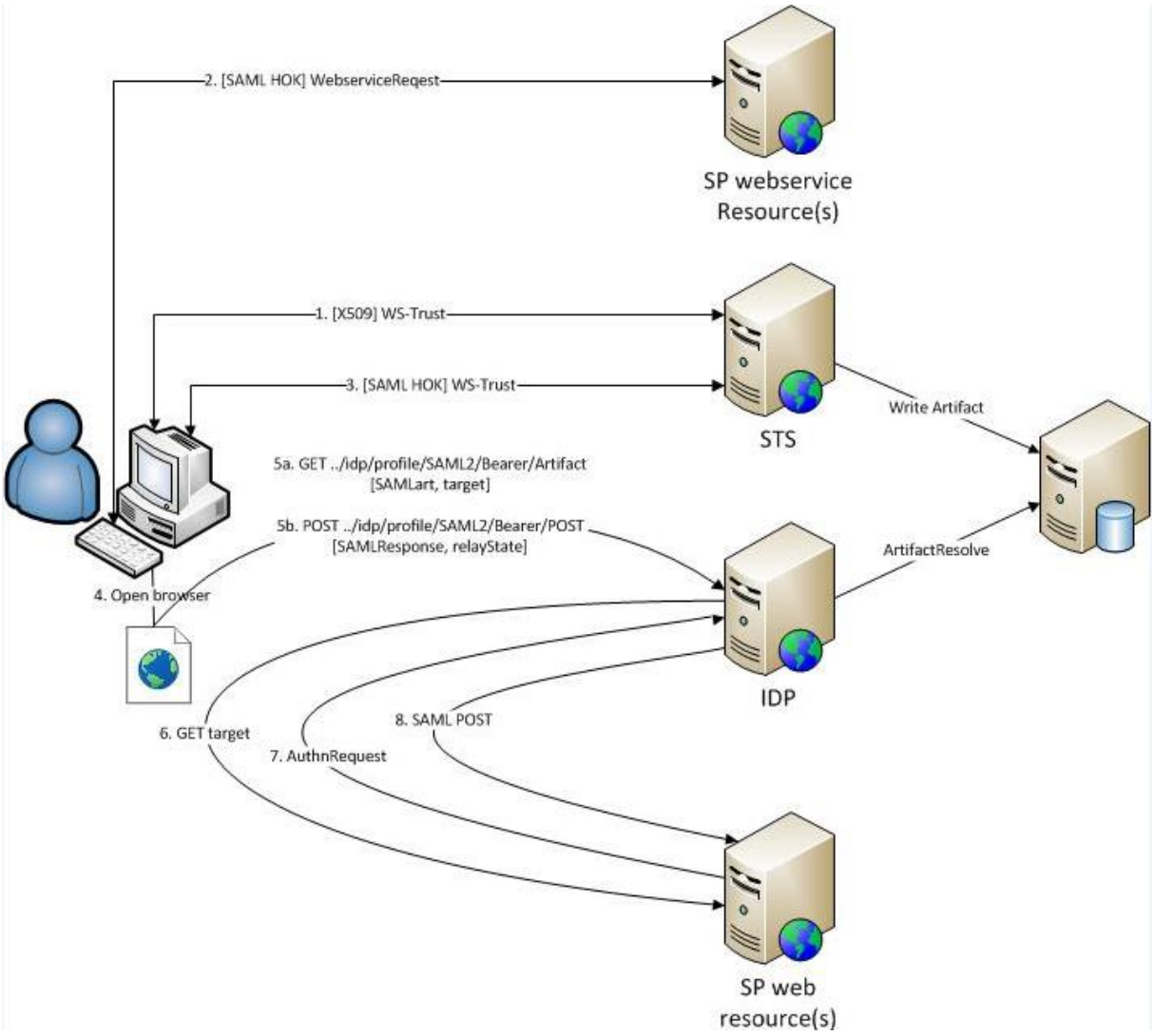
3.1.4 For business issues

- 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***For issues in production

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

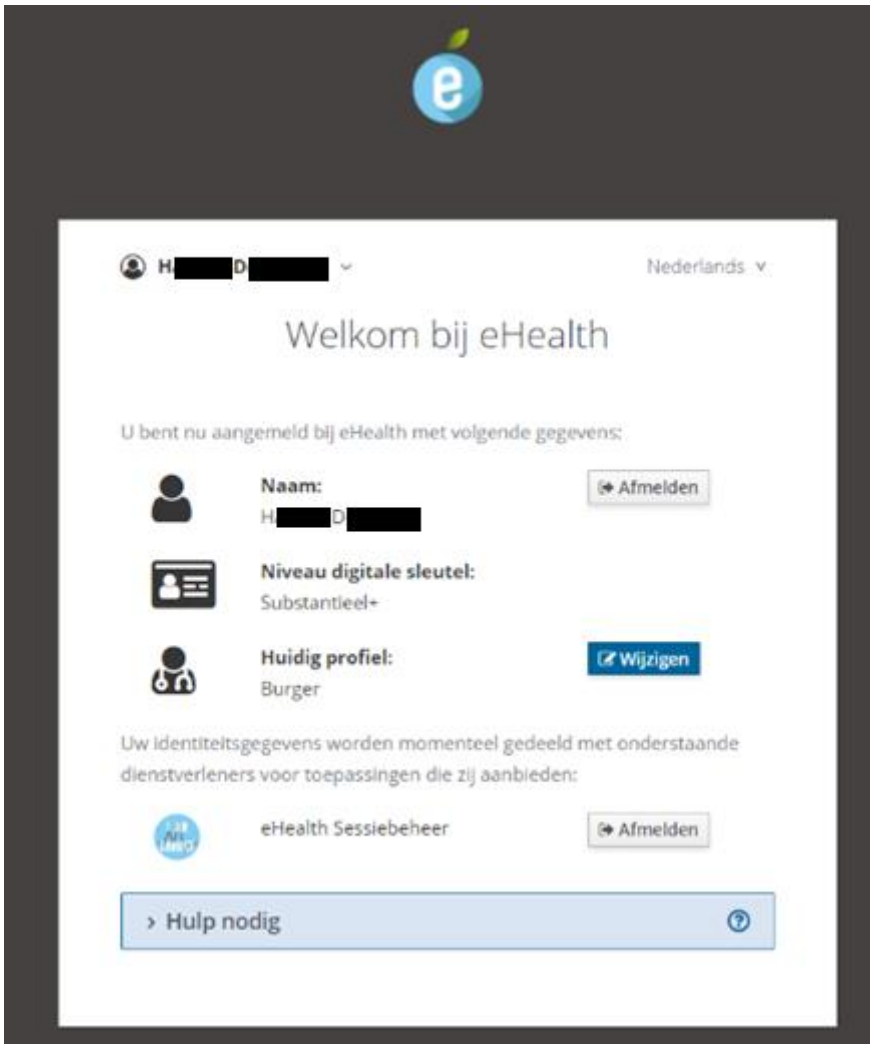


Note

All Request/Response messages are sent over SSL/TLS.

*The clientapplication **must** verify that direct communication with the eHealth Platform is setup, by verifying the certificate used by eHealth server in the SSL/TLS handshake.*

After validation of the Bearer Assertion, the IDP constructs the user's profile based on the contents of the Assertion and activates a session on his behalf.



As of this moment, the user will be able to access web applications in the eHealth I.AM Federation without the need to authenticate again.

If an HTTPRequest parameter 'RelayState' is present and points to a trusted location, the browser will not show the above page and automatically redirect the user to the given location.

Before the IDP will actually send authentication information on behalf of the user to a requested application, a notification will be shown (only once) on the 'confirm profile' page so the user can acknowledge that a browser session was started with his identity.

After confirmation, he is sent to the requested application (this is part of the normal process flow of browser SSO).


Aanmelden voor eHealthBox
Kies uw profiel:
Ik wil me aanmelden als:
Arts
Binnen de organisatie:
Kies een profiel
Profiel bevestigen
> Hulp nodig

5. Step-by-step

5.1 Steps 1-2: SSO web services (STS)

SSO is setup between WS hosted by the eHealth Platform or one of its trusted partners with eHealth I.AM STS as Security Token Service.

5.2 Steps 3-5: SSO Web services – Web App (STS → IDP)

SSO session for WS is transferred from fat to thin client.

5.2.1 Request Bearer Token from STS

The client sends a request to the STS to generate a new bearer token, based on the existing holder-of-key (HOK) token. The newly generated token will be valid for a short period (max 10 minutes).

There are multiple options to request this token, which will influence the result and remainder of the process flow.

See section 'Detailed solution steps' for details.

5.2.2 Open browser

A new or existing browser window is opened to setup SSO between the client's browser as thin client and eHealth IDP.

5.2.3 Authenticate at IDP

Depending on the result of step 3, the client uses his browser to send his authentication details to the eHealth IDP.

5.3 Steps 6-8: SSO Web App (IDP)

SSO is setup between web applications in the eHealth I.AM Federation with eHealth I.AM IDP as Identity Provider.

5.4 Detailed solution steps (Web services – Web App)

The eHealth platform offers two solutions to setup SSO from a fat to a thin client. Clients are free to implement one or the other.

5.4.1 Solution: GET Artifact

Using a fat client application and an active HOK Assertion (received from the STS at the start of the web service session), the user requests a reference to a Bearer Assertion in return. He will need to GET the reference to the eHealth IDP to get authenticated.

5.4.1.1 Step 3: Request Bearer Token from STS

The user sends a request to eHealth while using an active HOK Assertion as secure authentication token.

5.4.1.1.1 Endpoint URI

[ehealth environment] + /IAM/SingleSignOnService/v1:

- *PROD*: https://services.ehealth.fgov.be/IAM/SingleSignOnService/v1
- *ACC*: https://services-acpt.ehealth.fgov.be/IAM/SingleSignOnService/v1
- *INT*: https://services-int.ehealth.fgov.be/IAM/SingleSignOnService/v1

5.4.1.1.2 Inbound

- Header

WS-Security 1.1 SOAPHeader with following elements:

- *Timestamp*
- *SAML 1.1 Assertion*: active STS SAMLToken
- *Signature*: on timestamp and assertion

This is the same WS-SecurityPolicy as the one used in all eHealth Services protected with a samlToken.
Body

RequestSecurityToken (WS-Trust 1.3) with following info:

- *TokenType*: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
- *RequestType*: http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
- *KeyType*: http://docs.oasis-open.org/ws-sx/wstrust/200512/Bearer
- *AppliesTo*: eHealth IDP endpoint that will act as the resolver of the referenced Artifact ([ehealth environment]/idp/profile/SAML2/Bearer/Artifact)
  - *PROD*: https://www.ehealth.fgov.be/idp/profile/SAML2/Bearer/Artifact
  - *ACC*: https://wwwacc.ehealth.fgov.be/idp/profile/SAML2/Bearer/Artifact
  - *INT*: https://wwwint.ehealth.fgov.be/idp/profile/SAML2/Bearer/Artifact

Example (extract for readability)

Figure 1: Example SSO Artifact Request

5.4.1.1.3 Outbound

- Body

RequestSecurityToken Response(WS-Trust 1.3) containing a RequestedUnattachedReference with following info:

- *Reference*: URL that can be used in a browser to resolve the artifact.

- Example

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <wst:RequestSecurityTokenResponse Context="RC-3ea9c474-9539-4d0f-b0af-ea282fec1cb9" xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
            <wst:RequestedUnattachedReference>
                <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                    <wsse:Reference URI="https://wwwacc.ehealth.fgov.be/idp/profile/SAML2/Bearer/Artifact?SAMLart=AAQABPL...3A" ValueType="http://docs.oa
                </wsse:SecurityTokenReference>
            </wst:RequestedUnattachedReference>
        </wst:RequestSecurityTokenResponse>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Figure 2: Example SSO Artifact Response

5.4.1.2 Step 4-5: Open browser and authenticate at IDP

Note

The artifact is a hard-to-forge short-term reference for single-use only.

This means that the user has limited time to use it (a few minutes) and he can only use it once. If he tries to use it a second time, he will receive an error.

The client application opens the user's favorite browser with the URL from the reference received from the STS.

An optional HTTPRequest parameter 'RelayState' can be added to let the IDP redirect to a protected web application if authentication succeeds. To enable SSO from the STS token to web applications on a mobile, it could also be shown as a QR-code. Since the reference is a full URL, the mobile will automatically open up a browser and go to the URL.

- Example

5.4.2 Solution: POST Assertion

Using a fat client application and an active HOK Assertion (received from the STS at the start of the WS session), the user requests a Bearer Assertion in return. He will need to POST this Assertion to the eHealth IDP to get authenticated.

5.4.2.1 Step 3: Request Bearer Token from STS

The user sends a request to eHealth while using an active HOK Assertion as secure authentication token.

5.4.2.1.1 Endpoint URI

[ehealth environment] + /IAM/SingleSignOnService/v1:

- *PROD*: https://services.ehealth.fgov.be/IAM/SingleSignOnService/v1
- *ACC*: https://services-acpt.ehealth.fgov.be/IAM/SingleSignOnService/v1
- *INT*: https://services-int.ehealth.fgov.be/IAM/SingleSignOnService/v1

5.4.2.1.2 Inbound

- Header

WS-Security 1.1 SOAPHeader with following elements:

- *Timestamp*
- *SAML 1.1 Assertion: active STS SAMLToken*
- *Signature: on timestamp and assertion*

This is the same WS-SecurityPolicy as used in all eHealth Services protected with a samlToken.

- Body

RequestSecurityToken (WS-Trust 1.3) with following info:

- *TokenType: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0*
- *RequestType: http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue*
- *KeyType: http://docs.oasis-open.org/ws-sx/wstrust/200512/Bearer*
- *AppliesTo: eHealth IDP endpoint that will act as the consumer of the requested Assertion ([ehealth environment]/idp/profile/SAML2/Bearer/POST)*
  - *PROD*: https://www.ehealth.fgov.be/idp/profile/SAML2/Bearer/POST
  - *ACC*: https://wwwacc.ehealth.fgov.be/idp/profile/SAML2/Bearer/POST
  - *INT*: https://wwwint.ehealth.fgov.be/idp/profile/SAML2/Bearer/POST

Example (extract for readability)

```
<soapenv:Envelope xmlns:ns="http://docs.oasis-open.org/ws-sx/ws-trust/200512" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs
            <Assertion AssertionID="_477052849c6a7fbe6fd12540b761ad5a" IssueInstant="2018-10-19T14:17:27.923Z" Issuer="urn:be:fgov:ehealth:s
            <ds:Signature Id="SIG-D411B7B5889E507A3D153995889619137" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                <ds:SignatureValue>dWm0pOuNxdgvRmTpptI7fz0bQKviCdDhnvJ3QhT7jlMV+F2IOAQSpWpqrKxjkE8XWohLLqverCDg
                <ds:KeyInfo Id="KI-D411B7B5889E507A3D153995889619134">
            </ds:Signature>
            <wsu:Timestamp wsu:Id="TS-D411B7B5889E507A3D153995889618833">
        </wsse:Security>
    </soapenv:Header>
    <soapenv:Body wsu:Id="id-D411B7B5889E507A3D153995889619136" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurit
        <wst:RequestSecurityToken Context="RC-0f43d8be-322e-4a9c-8473-7308781f733e" xmlns:auth="http://docs.oasis-open.org/wsfed/authorizati
            <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
            <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
            <wst:KeyType>http://docs.oasis-open.org/ws-sx/wstrust/200512/Bearer</wst:KeyType>
            <wsp:AppliesTo>
                <wsa:EndpointReference>
                    <wsa:Address>https://wwwacc.ehealth.fgov.be/idp/profile/SAML2/Bearer/POST</wsa:Address>
                </wsa:EndpointReference>
            </wsp:AppliesTo>
        </wst:RequestSecurityToken>
    </soapenv:Body>
</soapenv:Envelope>
```

Figure 3: Example SSO POST Request

5.4.2.1.3 Outbound

- Body

RequestSecurityToken Response(WS-Trust 1.3) containing an Assertion with following info:

- *Issuer*: eHealth I.AM STS
- *Signature*: full Assertion is signed with eHealth I.AM certificate
- *Subject Confirmation*
  - *Method*: bearer
  - *NotOnOrAfter*: expiration time
  - *Recipient*: URL of consumer of this Assertion
- *Conditions*: short period of validity
- *AuthnStatement*: context used to authenticate to the STS at start of SSO Session
- *AttributeStatement*: attributes present in secure authentication token that was used to authenticate to the STS.

Example (extract for readability)

Figure 4: Example SSO POST Response

5.4.2.2 Step 4-5: Open browser and authenticate at IDP

Note

The Bearer Assertion is a short-term token.

This means that the user has limited time to use it (a few minutes).

To send the received Assertion to eHealth, it must be wrapped in a SAML 2.0 Response (SAML Web Browser SSO Profile).

```
<saml2p:Response ID="[SAMLResponseID]" IssueInstant="[SAMLResponseIssueInstant]"
Version="2.0" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
  [SAMLAssertion]
</saml2p:Response>
```

The client application must fill the [] fields dynamically with following data:

- [*SAMLResponseID*]: unique id for tracing and to prevent certain attacks. Type of this XSD attribute is ID. An xsd:ID value must be an NCName meaning it must start with a letter or underscore, and can only contain letters, digits, underscores, hyphens, and periods.
- [*SAMLResponseIssueInstant*]: time that the Response was generated to prevent certain attacks. Type of this attribute is dateTime. The type xsd:dateTime represents a specific date and time in the format CCYY-MM-DDThh:mm:ss.sss, which is a concatenation of the date and time forms, separated by a literal letter "T". All of the same rules that apply to the date and time types are applicable to xsd:dateTime as well. An optional time zone expression may be added at the end of the value.
- [*SAMLAssertion*]: the Assertion received in previous step. As the Assertion is signed by eHealth, do not change one bit to this element when inserting it in the Response element or the signature will get broken and the Assertion will become invalid.

After the SAML Response is generated, the client application opens with the user's favorite browser a local html file containing a form.

```
<form method="post" action="[ehealth environment]/idp/profile/SAML2/Bearer/POST">
   <input type="hidden" name="RelayState" value="[targetId]" />
   <input type="hidden" name="SAMLResponse" value="[response]" />
   <input type="submit" value="Submit" />
 </form>
```

The client application must fill the fields automatically before opening the file in the browser with the following data:

- [*ehealth environment*]: URL of IDP Assertion Consumer in same (!) environment where the Assertion was requested from the STS.
  - *PROD*: https://www.ehealth.fgov.be/idp/profile/SAML2/Bearer/POST
  - *ACC*: https://wwwacc.ehealth.fgov.be/idp/profile/SAML2/Bearer/POST
  - *INT*: https://wwwint.ehealth.fgov.be/idp/profile/SAML2/Bearer/POST
- [*targetId*]: target URL of the protected application the user wants to access (optional)
- [*response*]: SAMLResponse containing the received Assertion, encoded in Base64.

A typical implementation of html file should have an autosubmit function, an explanation and a backup solution in case the browser did not submit it automatically.

- Example

SAML 2.0 Response (extract for readability)

```
<saml2p:Response ID="_81e23b6b-c6e8-4810-87da-6379c60a1261" Version="2.0" IssueInstant="2015-04-15T09:47:27.312+02:00"
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="_9c295dc3845b488488b759b070eb781a" IssueIr
</saml2p:Response>
```

HTMLForm

```
<form method="post" action="https://www.ehealth.fgov.be/idp/profile/SAML2/Bearer/POST">
   <input type="hidden" name="RelayState" value="https://www.partner.fgov.be/secure" />
   <input type="hidden" name="SAMLResponse" value="PHNhb...zZT4=" />
   <input type="submit" value="Submit" />
 </form>
```

6. Test and release procedure

6.1 Procedure

This chapter explains the procedures for testing and releasing an application in acceptation or production.

6.1.1 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.

6.1.2 Development and test procedure

You have to develop a client in order to connect to our web service. Most of the info on how to integrate is published on the eHealth portal.

6.1.3 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. The eHealth platform suggests testing during a minimum of 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. The eHealth platform prepares the connection to the production environment and provides the partner with the necessary information. During the release day, the partner provides the eHealth platform with feedback on the test and performance tests.

For further information and instructions, please contact: ***integration-support@ehealth.fgov.be***.

6.1.4 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 the eHealth platform on the progress and test period.

6.1.5 The use of username, password and token

The username, password, and token are strictly personal.
Every user takes care of his username, password and token, and he is forced to confidentiality of it. It is prohibited to transfer them to partners and clients. Until inactivation, every user is responsible for every use, including the use by a third party.