Identity & Authorization Management (I.AM)
Logout
Technical specifications
Version 1.3

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	11/07/2018	eHealth platform	Initial version
1.1	27/06/2018	eHealth platform	Update
1.2	07/05/2019	eHealth platform	Update of IDP Logout for 20182
1.3	25/02/2021	eHealth platform	Review IDP screens (new look and feel)

2. Introduction

If you let users authenticate themselves to access a protected application, you should also take care of ending their authenticated session properly when they leave the application. This means you must offer them some form of "Logout".

A distinction should be made between a Local and a Global Logout:

1. Local Logout: authenticated user is disconnected from a given application. However, he remains authenticated in the IDP[1] where he submitted his credentials AND in all other applications he might have accessed during the same browser session.
2. Global Logout: authenticated user is disconnected from all applications and IDP in one click-action.

Closing all browser windows on the client ends the session (which logs out the user automatically) but better is that each application offers a logout button/link. This will not force the client to close all browser windows to make sure he is no longer authenticated in a web application.

Also important to notice, Local Logout in one application will not end the session in the IDP[2] that was used for authentication. When a user tries to authenticate again after a Local Logout, using the same browser session, he will not need to submit again his eID pin code, username/password …

In fact, that is what Single Sign On (SSO) is all about.

The IDP has itself a Logout link to end its own session properly with an option for the user to propagate logout to all applications for which he authenticated during that session.

[1] Identity Provider: party providing identity information on a current user

[2] Unless the browser is closed or the session timeout is expired.

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. Local Logout

Authenticated user is disconnected from a given application. However, he remains authenticated in the IDP where he submitted his credentials AND in all other applications he might have accessed during the same browser session.

Local Logout in one application will not end the session in the IDP (unless the browser is closed or the session timeout is expired) that was used for authentication. When a user tries to authenticate again after a Local Logout, using the same browser session, he will not need to submit again his credentials (eID/pincode, username/password, ...).

This logout must be used to allow user to switch profile without authenticating himself again.

4.1 Shibboleth Logout Service

4.1.1 Step 1: xml configuration

If the host is using Shibboleth, he should configure a Logout[3] or LogoutInitiator in the Shibboleth configuration file shibboleth2.xml.

Version 2.4+

```
<Logout>Local</Logout>
```

Older versions

```
<LogoutInitiator type="Chaining" Location="/Logout" relayState="cookie">
  <LogoutInitiator type="Local" return="URL_AFTER_LOGOUT"/>
</LogoutInitiator>
```

The location can be chosen freely.

The return value “URL_AFTER_LOGOUT” must be a valid URL accessible by the user’s browser, as it will be used to redirect the user after Logout is performed.

4.1.2 Step 2: html link

The protected web application should have some kind of link launching a GET request of following form:

[scheme]://[hostname]/[handlerURL]/[Location]?return=[returnURL]

Scheme	https (you should not use ‘http’ for protected applications)
Hostname	Host name of the webserver making the protected application available for your users.
handlerURL	By default /Shibboleth.sso but in fact it depends on what is defined as handlerURL for the protected application in shibboleth2.xml (could be totally different)
Location	By default, ‘/Logout’. Taken from the Location attribute in the LogoutInitiator configuration in shibboleth2.xml, see example in step 1 (‘/Logout’).
returnURL	HTTP Request Param "return" is optional. If not present the user will be redirected after logout to the URL defined in the LogoutInitiator return attribute in shibboleth2.xml.

[3] *See the ‘eHealth IAM – Shibboleth SP’ cookbook for more information on configuration of the Logout element*

5. Global Logout

With this method of logout, the authenticated user is disconnected from the IDP and the IDP propagates eventually the logout to all applications accessed during the user's active session.

If the SP protecting an application does support SAML 2.0 Logout Profile, the preferred way to logout the user is to use that profile. There are 2 options to get the logout page for the IDP:

- Send the user with an HTTP GET to the 'Simple' Logout URL. This will trigger logout in the IDP itself and eventually propagate Logout to all SPs involved in the user's session, including the application that sent the user to the Logout URL.
- Trigger the logout locally in the application and POST a SAML 2.0 LogoutRequest to eHealth's SLO Logout URL (defined in eHealth's SAML 2.0 Metadata IDPSSODescriptor, available online).

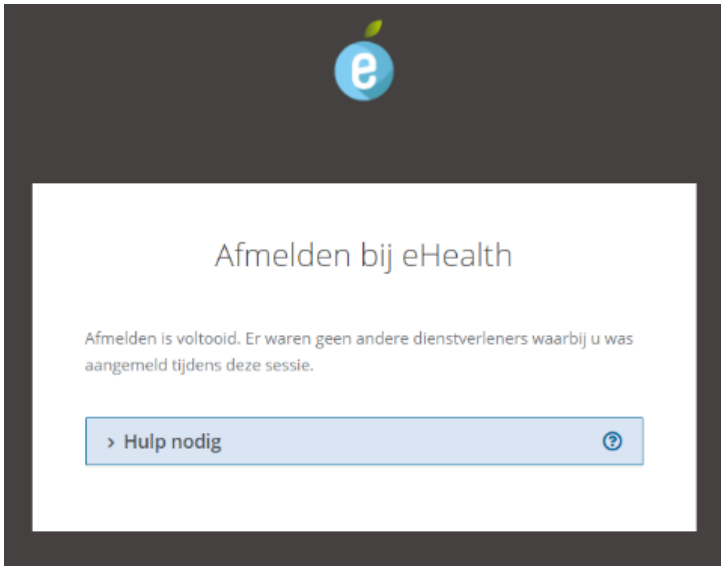
5.1 Logout procedure

The IDP, used to authenticate the users and transmit identity information to the SPs hosting applications, offers two ways of contacting the logout procedure : SAML 2.0 Single Log Out Profile or the simple Logout url.

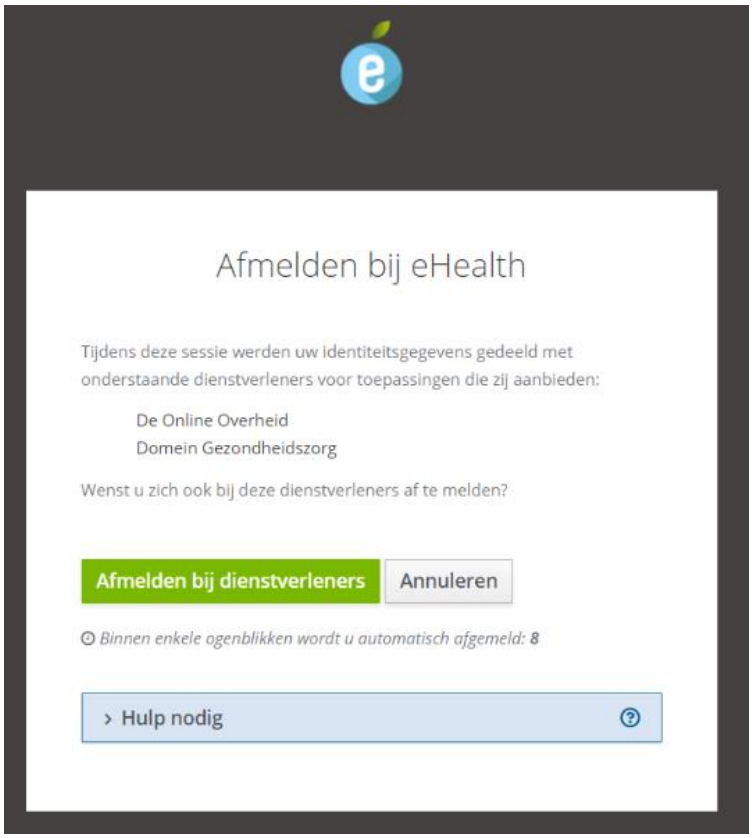
In both cases, one or more pages can be shown and logout can end with a redirect back to the requesting application or it can end on a logout status page at eHealth (default setup).

Unless the user chooses explicitely not to, eHealth will try to propagate logout to the service providers of all applications for which the user authenticated during the session (if any).

In case the user did not complete access to any application, no propagation will take place.



In case he did access some applications, propagation of logout will be proposed.

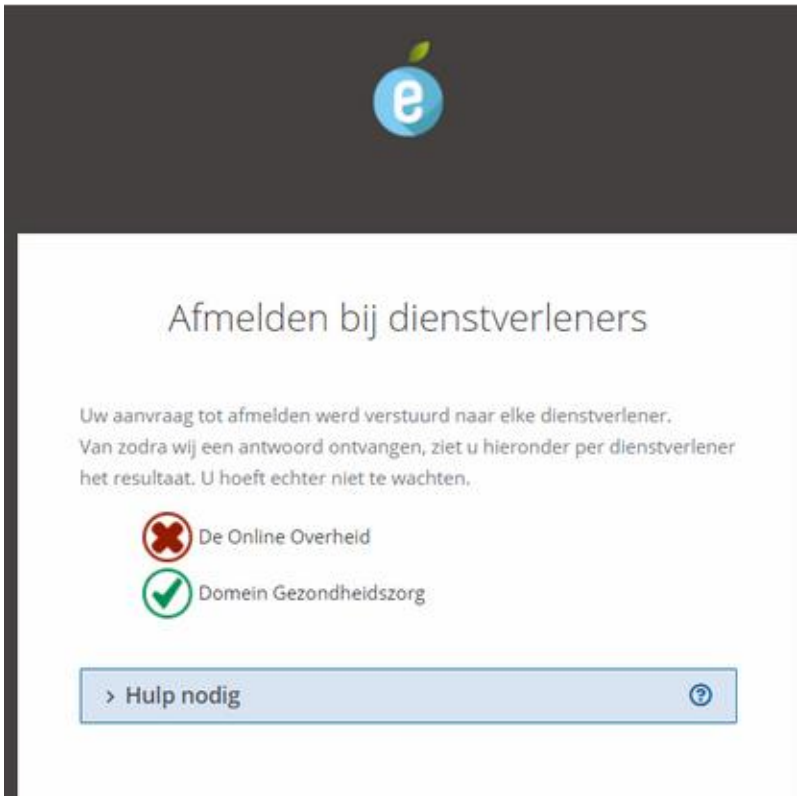


The user can cancel the logout propagation, he can however not cancel logout completely. Logout at eHealth IDP itself is already performed.

If he does not cancel propagation, eHealth propagates logout by sending a SAML 2.0 Single Logout Request to each Service Provider for which assertions were sent during the user's session.

The result is a red cross or a green check mark.

Status per Service Provider starts with a red cross and after a few seconds a green check mark may appear.



Session Duration

With Web SSO (IDP), each web app determines its session duration and that is completely separate from the generated session token that is only used to pass the authentication data from the IDP to the SP.

With the IDP, the maximum duration is 1 hour of inactivity (no request from the browser to the IDP webapp).

For each application (Service Provider), if you want to support the SLO, you must provide us the SingleLogoutService location (the location **must be** 'https://...' and not 'http://...') and the binding (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST is the best option) for your application.

In order to get a green check mark, the SP needs to support SAML 2.0 SLO and it must return a success status.

Otherwise, a red cross will remain.

If the SP is configured to get the SAML Response in the browser window (for SAML 2.0 SLO only – see 5.3) or if the SP requested explicitly to redirect the user after logout (to an url from a trusted host), the user will not remain on the logout status page. The user will remain just a few seconds on the logout page so the SLO requests can be sent to each SP. The user will not wait for the responses but that is OK.

By default, eHealth responds to SAML 2.0 SLO Requests by responding in a hidden iframe. That makes it possible to respond to the SP (requirement of the profile) AND to show the status page of eHealth logout.

It is possible to configure a SP to get the SAMLResponse back in the browser's window so it gets control back to do whatever it wants to do to complete logout flow on its side. A special setting may occur in eHealth IDP metadata for this SP.

5.2 'Simple' Log Out URL

As detailed before, there are two ways of getting the logout page for the IDP.

The first one is to perform a HTTP GET on the following logout URL

[idp-root[4]]/profile/Logout.

Logout with redirection:

The Logout URL has an optional parameter: **return.**

[idp-root]/profile/Logout?return=[URL to redirect]

This parameter is made to trigger an automatic redirect after 5 seconds at the specified URL.

If the parameter is not used, the page will remain open with the logout results.

Note: The domain of the hostname of the URL must be known to eHealth to be trustworthy in order to prevent phishing attacks.

If you want to register your domain as trusted, please contact eHealth[5].

5.3 SAML 2.0 Single Logout

The other way of logging out is to trigger the SAML2 single logout from the application by performing a POST request on eHealth's SLO URL

[idp-root[6]]/profile/SAML2/POST/SLO.

The end-user will also be lead to the IDP logout page. The only difference is in the fact that this is a signed SAML POST and you'll receive a signed SAML response instead of an HTTP GET.

If the host is using Shibboleth, he should configure it to send a SAML2 Logout via the Shibboleth configuration file shibboleth2.xml.

```
<Logout>SAML2</Logout>
```

If SAML 2.0 Logout Profile is not supported

If the SP protecting an application does not support SAML 2.0 Logout Profile, logout can still be achieved using following procedure:

In the Local Logout URL of the protected application, the return parameter must be set to the 'Simple' Logout URL of the IDP. (i.e [idp-root]/profile/Logout).

This way, the user will be disconnected from the protected application before being redirected to the IDP where he will also be disconnected.

It is possible to give this second URL also a return parameter in order to redirect once more after IDP logout is performed to a location of their choice (if the IDP trusts it).

Remark: You should use URL encoding to prevent errors.

[4] *Idp-root depends on the environment used for integration with eHealth's IDP. For production, this is* ***https://www.ehealth.fgov.be/idp***

[5] *For contact details, see chapter 3*

[6] *Idp-root depends on the environment used for integration with eHealth's IDP. For production, this is* ***https://www.ehealth.fgov.be/idp***