

**Identity & Authorization Management (IAM)
Identity Provider (IDP)
Technical specifications
Version 1.3**

This document is provided to you free of charge by the

eHealth platform

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

All are free to circulate this document with reference to the URL source.

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 Identity	5
2.3 Trust	6
2.3.1 Web SSO	6
3. Support	7
3.1 For issues in production	7
3.2 For issues in acceptance	7
3.3 For business issues	7
3.4 Certificates	7
4. Identity	8
4.1 Authentication method (default authenticator)	8
4.1.1 Belgian identity card	11
4.1.2 ItsMe	11
4.1.3 Username and password	11
4.1.4 Security code mobile app	11
4.1.5 Helena	12
4.1.6 Belgian citizen token	12
4.2 Multiple authentication provider	12
4.3 Subjects, Principals and Profiles	14
4.4 Attributes	15
4.4.1 Identity	15
4.4.2 Certified	16
4.4.3 Transport	16
5. Authorization	17
5.1 Model	17
5.1.1 Role-based	17
5.1.2 Attribute based	17
5.2 Levels	17
5.2.1 Unauthenticated	17
5.2.2 List of identities (user profiles)	17
5.2.3 Access Rules Policy	18
5.2.4 Attribute Filter Policy	18
5.2.5 Final decision	18
6. Web Browser SSO Profiles	23
6.1 SAML 2.0	23
6.1.1 HTTP POST	23



6.1.2	HTTP-POST pull.....	25
6.1.3	HTTP-Artifact.....	26
6.1.4	urn:mace:shibboleth:2.0:profiles:AuthnRequest.....	28
6.2	SAML 1.1	28
6.2.1	Browser/POST	30
6.2.2	Browser/POST pull	30
6.2.3	Browser/Artifact.....	32
7.	Configuration options	33
7.1	Metadata@eHealth.....	33
7.2	SP AuthnRequest.....	34
7.2.1	HTTP Request Parameters.....	34
7.2.2	SAML 2.0 AuthRequest.....	34
8.	Risks and security	36
8.1	Risks & safety	36
8.1.1	Web SSO.....	36
8.2	Security	36
8.2.1	Business security	36
9.	Test and release procedure.....	37
9.1	Procedure.....	37
9.1.1	Initiation	37
9.1.2	Development and test procedure	37
9.1.3	Operational follow-up	37
10.	Error and failure messages.....	38
10.1	Info	38
10.2	Warning.....	38
10.3	Errors.....	39
10.3.1	Request rejected	39
10.3.2	Unexpected error	40
10.3.3	User errors	41

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



1. Document management

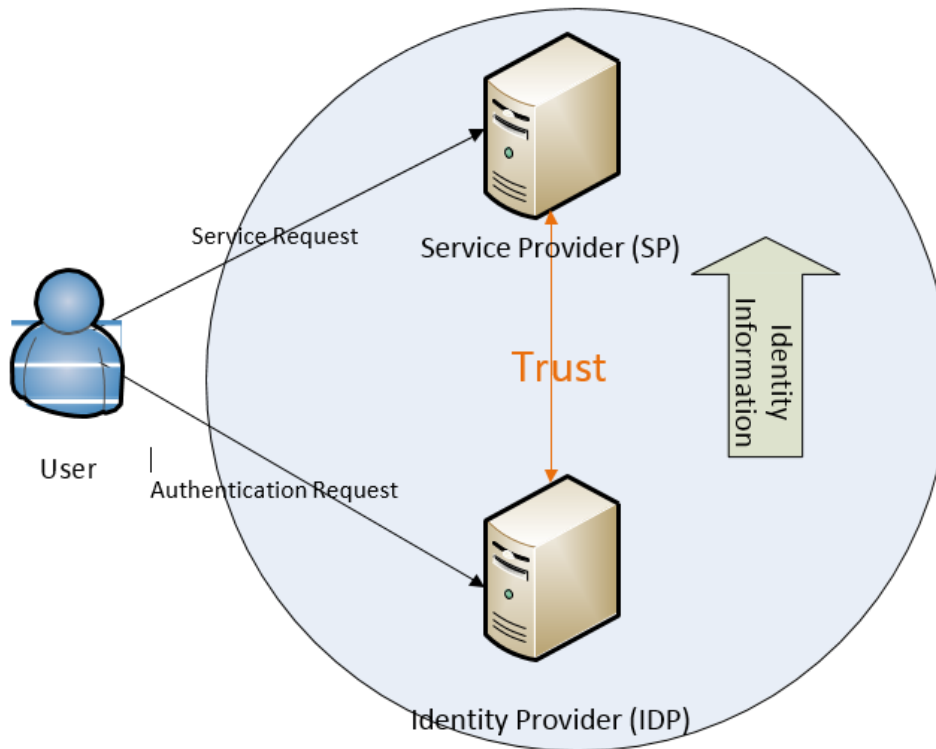
1.1 Document history

Version	Date	Author	Description of changes / remarks
1.0	11/02/2013	eHealth platform	Initial version
1.1	13/05/2019	eHealth platform	Review IDP screens (new look and feel)
1.2	16/03/2020	eHealth platform	Review for 2020.1 and new versioning
1.3	24/02/2021	eHealth platform	Review

2. Introduction

2.1 Goal of the service

The eHealth I.AM Identity Provider (IDP) provides Identity and Authorization Information to Service Providers (SP) on behalf of users who are authenticated at the IDP and wish to get access to a service hosted at the SP.



2.2 Identity

- An identity, in the domain of cross enterprise communication over internet, can be defined as a set of data that uniquely describes a person or a thing (sometimes referred to as subject or entity).
- A critical problem in the online world knows with whom you are interacting.
- To determine the identity of a user, different authentication methods can be used to challenge the user to prove who he pretends to be.
- Users can also have multiple digital identities: as a physical person, as a professional in healthcare (HC), as a representative of an organization, etc.
- An IDP will typically provide one or more authentication methods and have access to one or more authentic sources to search for identities associated with the user.
- Different sets of data will form those identities. These data elements are also called attributes associated to the identity.
- On request, an IDP may provide identity information on behalf of the user to an SP.
- In respect of the user's privacy, the SP and IDP will establish a security context in which it is safe to transfer data on his behalf and this data should only be the set of attributes required by the SP to grant the user access to its protected application.
- A trust relation between SP and IDP will be setup for this purpose.

- Multiple SPs can setup this trust with one IDP to realize SingleSignOn (SSO) between applications protected by those SPs as the IDP will request the user to authenticate only once after which he remains known to the IDP for the duration of the session.

2.3 Trust

The IDP only accepts authentication requests for services at known SPs.

SPs need to be registered in the eHealth I.AM Federation to establish a trust relation so both parties know how to setup a secure conversation and what data to transfer.

2.3.1 Web SSO

- Web SSO means that, during one web browser session, the user only needs to authenticate once at the IDP. He may request access to multiple services from multiple SPs while his session remains active without the need to re-authenticate.
- The IDP supports multiple authentication methods for this purpose. They are listed in the section 'Authenticationmethod'.
- Once authenticated, users can choose from different profiles (principals), each representing a different aspect of their identity as known to the IDP.
- The IDP can perform access rules based on the current profile, chosen by the user, and the application for which he is requesting access. The result of those access rules will be sent to the SP.
- On behalf of the user, the IDP will only send to the SP the identity and authorization information that SPs requires to know. For this purpose, multiple SSO Profiles are supported to allow different types of SPs to integrate with the eHealth I.AM Federation establish a trust and communicate with the IDP.
- You will find them listed in the section 'Web Browser SSO Profiles'.



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. Identity

4.1 Authentication method (default authenticator)

The eHealth IDP supports different levels of authentication to offer users multiple options to authenticate themselves.

eHealth IDP relies on BOSA FAS (Federal Authentication Service).

Each authentication method comes with a security level as one method is more secure than the other. To each application, protected by the eHealth IDP after its registration in the eHealth I.AM Federation, a minimum security level is attached. When a user presents himself to authenticate for a given application, the eHealth IDP will only offer those authentication methods, which apply to the minimum security level as demanded by the application.


Three levels are defined :

- Low (username/password)
- Substantial (TOTP, Helena)
- High (ItsMe, eID)




Kies uw digitale sleutel om aan te melden [Hulp nodig?](#)

Digitale sleutel(s) met **eID** of **digitale identiteit**




AANMELDEN
met eID kaartlezer




AANMELDEN
via itsme

[Je itsme-account aanmaken](#)


Digitale sleutel(s) met **beveiligingscode** en **gebruikersnaam + wachtwoord**




AANMELDEN
met beveiligingscode via e-mail



AANMELDEN
met beveiligingscode via mobiele app




AANMELDEN
met Helena



AANMELDEN
met beveiligingscode via token

Digitale sleutel(s) met **gebruikersnaam + wachtwoord**





AANMELDEN
met gebruikersnaam en wachtwoord

Figure 1: Security level set to minimum Low (Dutch view)

Choisissez votre clé numérique pour vous identifier. [Besoin d'aide?](#)

Clé(s) numérique(s) avec l'eID ou identité numérique

 IDENTIFICATION avec un lecteur de cartes eID	 IDENTIFICATION via itsme
--	--

[Créer votre compte itsme](#)

Clé(s) numérique(s) avec code de sécurité et nom d'utilisateur + mot de passe




 IDENTIFICATION avec un code de sécurité envoyé par e-mail	 IDENTIFICATION avec un code de sécurité via une application mobile
 IDENTIFICATION avec Helena	

Figure 2: Security level set to minimum Substantial (French view)

As the eHealth IDP offers SSO, a user only needs to authenticate once in a web browser session. However, if he tries to access another application, which requires a higher security level than provided by the authentication method already used during the session, he will be forced to re-authenticate using one of the authentication methods that provide the new minimum security level.

Aanmelden voor eHealthBox

Kies een beheerder om verder te gaan:



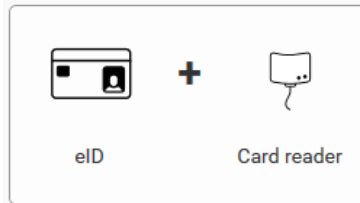
 U bent reeds aangemeld maar deze toepassing vereist dat u zich aanmeldt met een veiligere manier om u te identificeren. 

Figure 3: Higher security level: Authentication methods (Dutch view)

The authentication methods supported by eHealth IDP are listed below.

4.1.1 Belgian identity card



The electronic identity card, or eID, is the legal identity card in Belgium. The eID works with a PIN code and contains a microchip with additional information that is not visible on the card: your address and 'digital certificates'. These certificates confirm your identity when you use online applications. This is the strongest authentication method supported by the eHealth IDP (security level High).

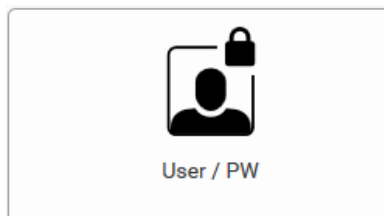
4.1.2 ItsMe



In addition to the digital keys offered by the government, there are also other parties that may offer digital keys allowing citizens to log into online government services.

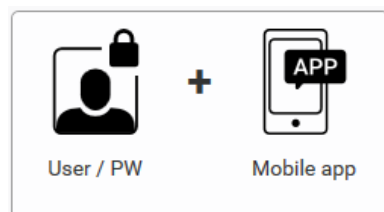
Currently there is one authorized partner: Itsme®, a service offered by Belgian Mobile ID. More information about Itsme® is available at www.itsme.be (security level High)

4.1.3 Username and password



This is a simple username and password combination. This is the least strong authentication method supported by the eHealth IDP (security level Low).

4.1.4 Security code mobile app



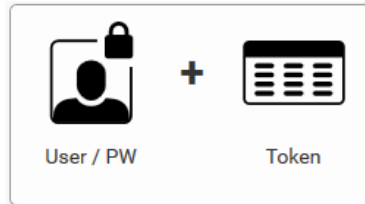
This digital key requires your user name and password in combination with a security code (security level Substantial).

4.1.5 Helena



Helena is a digital key that allows you to log in to the eHealth applications as a patient. (security level Substantial)

4.1.6 Belgian citizen token



This token is a card the size of a bankcard containing 24 personal codes. You can use these codes to boost the security of a username and password authentication. You will be prompted for one of the 24 personal codes on your card after you have authenticated with username and password. This is a strong authentication method supported by the eHealth IDP (security level Substantial).

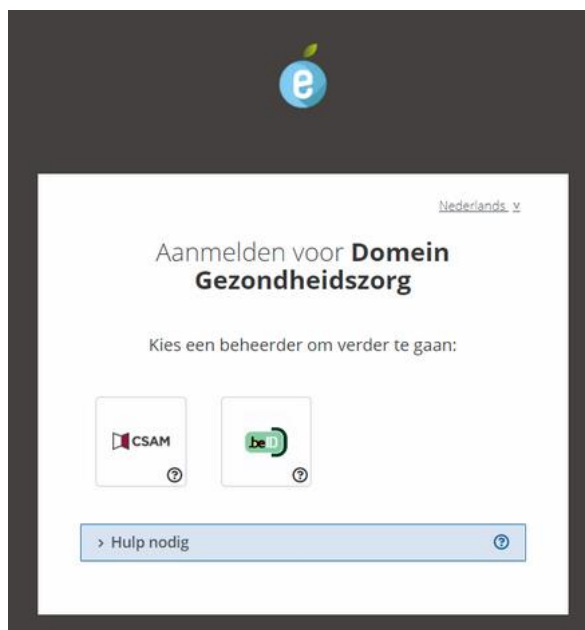
This authentication method will soon be removed from the list of available authentication methods on eHealth platform.

4.2 Multiple authentication provider

Some applications may require the use of other authentication methods than the default one. A choice will be shown to the user if a choice needs to be made.

In production, most applications are configured for authentication by CSAM FAS and therefore the page will not appear in SSO requests for those applications. The user will be redirected to FAS automatically.

Up to acceptance or in case of 'eid fallback' (i.e. FAS unavailable), we offer our internal eID authenticator as alternative and therefore the page will appear so the user can make his choice of provider.

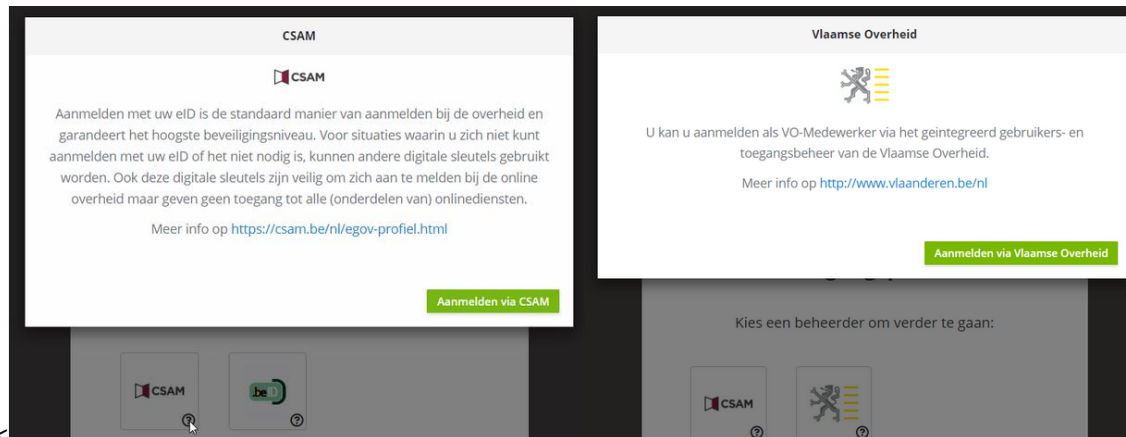


Some applications have other providers to choose from :



Clicking on a tile redirects the user to the chosen provider.

Clicking on the question mark in the bottom-right corner of each tile opens a modal with more info and an option to login with that provider.



4.3 Subjects, Principals and Profiles

The eHealth IDP uses ‘principals’ and ‘subjects’ to hold information on users.

A principal is an identity assigned to a user because of authentication. A subject is a container for authentication information, including principals. Each principal stored in the same subject represents a separate aspect of the same user's identity, much like cards in a person's wallet. (For example, an ATM card identifies someone to their bank, while a membership card identifies them to a professional organization to which they belong.)

Once the user has authenticated by submitting his credentials, the IDP will create a basic identity for the user (SSIN, first name, last name) which will remain known throughout the duration of the web browser session. The user will not need to submit his credentials again. They will be stored as a principal in the subject mapped to the current user. With this basic principal, the eHealth IDP will enrich the subject of the user by searching for other applicable identities of the user in the eHealth Authentic Sources. All retrieved identities are stored as principals in the subject mapped to the current user. The list of retrieved principals will be presented to the user and he will be requested to choose which identity he wants to use for the application he is trying to access. If the user tries to access more than one application during the same web browser session, he will be presented with this choice once for each application as he might want to choose different identities for different applications. The latest identity is kept as the active one in the session and will be presented by default on a subsequent authentication request. The list of identities may vary on each authentication request as the eHealth IDP will only present identities that are applicable for the application the user is trying to access.

For this purpose, all principals are divided into profiles. The eHealth IDP supports 5 profiles:

- Citizen: for the principal with the basic authentication if the user wants to identify himself as a natural person. This is the default profile when a user authenticates on the eHealth IDP.
- Quality: for the principals that identify the user as a professional (e.g. DOCTOR)
- Organization: for the principals that identify the user as a representative of an organization he belongs to
- Mandate: for the principals that identify the user as the mandatary of another person or organization from whom he has received a mandate to act on their behalf
- Parent : for the principals that identify the user as a parent who has filiation for a child.

For each application registered in the eHealth I.AM Federation, the IDP knows which type of profiles may be applicable and will only search for those in the Authentic Sources of the eHealth platform.

Only the identities of one of the supported and applicable profiles will be presented to the user to choose from



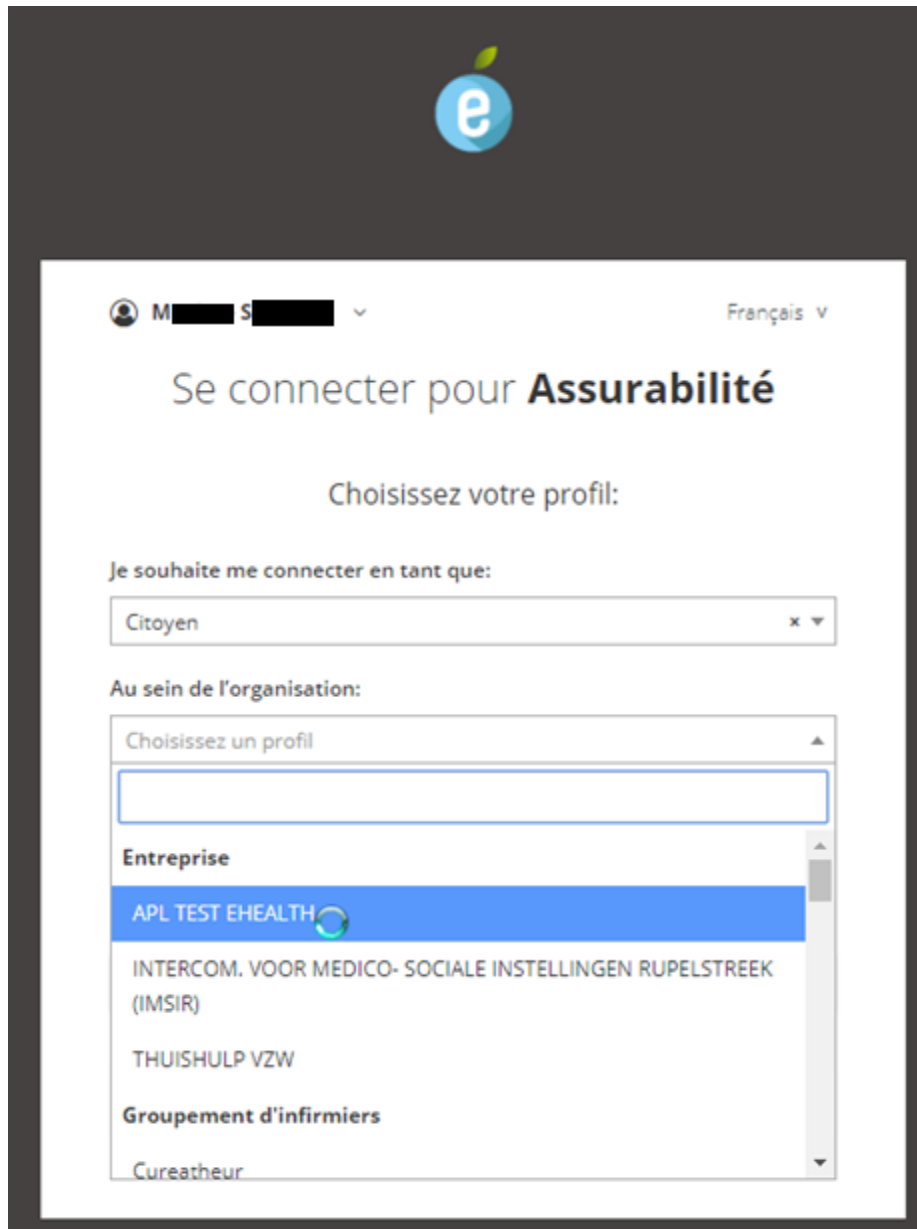


Figure 4: Profiles (French view)

4.4 Attributes

4.4.1 Identity

To send data about a chosen identity to an SP, the IDP uses attributes. These can be anything that the IDP knows about the user and that may be helpful to the SP. Some examples of this type of data are:

- the user's name
- specific certifications a user possesses
- information about the user's role in an organization specific privileges a user has been granted.

Each identity of the user is composed out of a list of attributes. For each type of profile, a different set of attributes will form this identity.



For a list of all supported identity attributes, what they mean and in which type of profile they are present, please consult the document ‘eHealth I.AM – Federation Attributes’¹.

4.4.2 Certified

Next to the authentication attributes that together form the identity chosen by the user, SP may require additional information of their users.

eHealth platform DP will resolve those by querying the eHealth platform Authentic Sources. These are called certified attributes as the eHealth platform certifies them.

To respect the user’s privacy, SPs must define during registration which additional attributes they require about their users for each protected application requestable by their users. An Attribute Release Policy will control that only those additional attributes will be sent to the SP.

4.4.3 Transport

How exactly these attributes are sent to the SP, is defined by the Web Browser SSO Profile, initiated by the SP. See ‘Web Browser SSO Profiles’ for the list of supported profiles and an explanation of how they are used.

¹ <https://www.ehealth.fgov.be/ehealthplatform>



5. Authorization

As the name I.AM (Identity & Authorization) suggests, eHealth I.AM is more than just Identification. In the process, also a part “Authorization” can be involved.

The eHealth IDP can be integrated in multiple authorization models and perform authorization at different levels.

5.1 Model

Authorization can be approached in different ways. eHealth IDP supports the following models.

5.1.1 Role-based

Access to a resource can be secured, based on the role membership of the user requesting access. Roles can be used to partition your application’s user base into sets of users that share the same security privileges within the application. A role of AdminUser for example could grant a user more rights in the target application. For this purpose, the eHealth IDP can execute an Access Rules Policy that will result in zero to many roles attributed to the principal. These roles will be included as an identity attribute in the response from the IDP to the SP.

5.1.2 Attribute based

Also known as claim-based or identity-based access control.

This is an extension on the role-based authorization model where claims are added to the principal as identity attributes. These claims can be compared with a set of authorization policies for the target application. A claim of isDoctor=true for example could grant doctors more rights than patients in a target application.

For this purpose, the eHealth IDP can request certified/claim attributes in its authentic sources and sent them, along with the basic identity attributes, to the SP.

5.2 Levels

When a user requests access to a protected application at an SP, there are multiple levels of authorization involved between the request of the unauthenticated user to access the application at the SP, the authentication process at the IDP and the final access to the application.

As each SP can host one or more applications in his own domain, this becomes a shared responsibility between the eHealth platform and the partner.

5.2.1 Unauthenticated

Unauthenticated users requesting access by using their browser to get to the application’s URL, must be stopped by the SP and redirected to the eHealth IDP for authentication. Therefore, the SP must use one of the supported Web Browser SSO Profiles as explained in section ‘Web Browser SSO Profiles’.

5.2.2 List of identities (user profiles)

When one of the presented methods authenticates the user, a list of identities (each entity containing a set of attributes²) is collected by querying the Authentic Sources² of the eHealth platform.

Only the user’s identities applicable³ for the current application will be presented to choose from as it makes no sense that a user chooses an identity of which is known that access will be denied.

² See ‘Attribute-Based’ authorization model

³ Upon agreement, this filter can be disabled for one or more applications, in which case eHealth will offer ALL



This means:

- Identities of a profile-type that is not listed as supported by the application will not be queried for.
- Retrieved identities of profile type 'organization' will be filtered out unless the current application is registered as authorized for the given organization in the eHealth platform Authentic Source of Organizations.
- Retrieved identities of profile type 'mandate' will be filtered out unless the current application is registered as authorized for the given mandate in the eHealth Authentic Source of Mandates

5.2.3 Access Rules Policy

For each application, the eHealth platform defines a policy containing one or more Access Rules. The chosen identity will be run through a policy engine that will execute⁴ the access rules for the current application on behalf of the current identity. The outcome will be a decision to 'Permit' or 'Deny' access to the user based on the chosen identity. If the outcome was 'Permit', one or more 'roles' will be attributed to the chosen identity which may give him additional (or less) rights for specific actions in the target application.⁵

5.2.4 Attribute Filter Policy

On registration of a new SP or application, the eHealth platform defines a filter policy to prevent applications protected by an SP from seeing data that violates the policy. This policy will take in consideration the selected profile and the decision of the Access Rules Policy. The set of attributes that has been prepared so far for the requesting SP will be run through the filtering engine to decide the restricted set of attributes, which should be published to the SP. Only the set of attributes returned by the filtering engine will be added to the response of the IDP to the SP.

5.2.5 Final decision

Upon receipt of the IDP's response, according to the profile, the SP must verify that the response is valid, untampered and certified by eHealth IDP.

If not all conditions are met, the SP must reject the message and deny access.

If all conditions are met, the SP can retrieve attributes from the response as he wishes. He can ignore those that are of no interest to him.

5.2.5.1 Attributes

For this purpose, the authorization decision of the eHealth platform is sent by the IDP using some extra identity attributes⁶ in the response to the SP.

'urn:be:fgov:ehealth:1.0:authz-decision'

- Sent: Optional, i.e. always unless the Access Rules Engine was disabled for that particular application in which case it is entirely up to the hosting partner to verify access for the application
- Possible values:
 - Permit': based on the rules executed by the eHealth platform, current user is authorized to access the application.
Action: SP MAY execute additional access controls before access is granted or denied.

the organizations and/or mandates linked to the identified user.

⁴ Upon agreement, the Access Rules Engine can be disabled for one or more applications, in which case eHealth will NOT take an authorization decision.

⁵ See 'Role-based' authorization model.

⁶ You can also find them in the document 'eHealth I.AM – Federation Attributes', available on the eHealth Portal.



- 'Deny': based on the rules executed by the eHealth platform, current user is not authorized to access the application.
Action: SP MUST refuse access to the user.
- 'Indeterminate': for some reason, the eHealth platform could not take a decision to permit or deny access.
Action: SP SHOULD refuse access to the user unless it has valid reasons to expect an Indeterminate decision by the eHealth platform in which case it MUST execute itself sufficient access rules to take an appropriate decision.

'urn:be:fgov:health:1.0:role'

- Sent: Optional, i.e. only if attribute 'urn:be:fgov:health:1.0:authz-decision' equals 'Permit'
- Possible values: one or more roles (string), known in the eHealth Identity & Authorization System as stated in the 'DU' of the target application)

'urn:be:fgov:health:1.0:health-ref'

- Sent: Optional
- Possible value: a unique identifier for the current authentication session of the user in the eHealth IDP.

5.2.5.2 Authorization Decision Statement

Upon agreement with the partner, the eHealth IDP can⁷ be configured to include a separate authorization decision statement in the response with respect to the SAML Specifications:

- SAML 1.1: AuthorizationDecisionStatement
- SAML 2.0: AuthzdecisionStatement

The possible values of the Decision attribute are the same as in previous section.

Example: SAML 2.0 Assertion including an AuthzDecisionStatement

```
< saml2:Assertion ID=" 058c856afe86a1bf325e4387b152f40a" IssueInstant="2013-06-2:56:54.967Z" Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://idp.smals-mvm.be/shibboleth</saml2:Issuer>
  <ds:Signature>...</ds:Signature>
  <saml2:Subject>...</saml2:Subject>
  <saml2:Conditions>...</saml2:Conditions>
  <saml2:AuthnStatement>...</saml2:AuthnStatement>
  <saml2:AttributeStatement>...</saml2:AttributeStatement>
  <saml2:AuthzDecisionStatement Decision="Permit" Resource="urn:health:test:sso">
    <saml2:Action
      Namespace="urn:oasis:names:tc:SAML:1.0:action:ghpp">GET</saml2:Action>
    <saml2:Action
      Namespace="urn:oasis:names:tc:SAML:1.0:action:ghpp">POST</saml2:Action>
  </saml2:AuthzDecisionStatement>
</ saml2:Assertion >
```

5.2.5.3 Access denied by the eHealth platform

When a user must be denied access based on the rules that the Health platform executed itself, different strategies are possible for publication of this decision.

The eHealth platform offers the following publish-on-deny policies:

- SAML AttributeStatement/AuthzDecisionStatement

This is the default policy. A SAMLToken is returned including an AttributeStatement with the 'urn:be:fgov:health:1.0:authz-decision' attribute and optionally⁸ an AuthzDecisionStatement. See previous section for more details.

⁷ By default disabled: only be enabled for standard SAML 1.1 and SAML 2.0 POST and Artifact SSO Profiles.

⁸ Only for SAML 2.0 Profiles



- SAML Status Code

This is the default policy. A SAMLToken is returned including an AttributeStatement with the 'urn:be:fgov:health:1.0:authz-decision' attribute and optionally⁹ an AuthzDecisionStatement. See previous section for more details.

<StatusCode> of type Responder, optionally a second level <StatusCode> with value 'urn:be:fgov:health:1.0:status:xacml:decision:Deny' and a <StatusDetail> element with more detailed information on the 'Deny' decision.

The <StatusDetail> contains an <XACMLAuthzDecisionStatement> as defined in the SAML 2.0 Profile of XACML¹⁰ with structured information on the decision, the subject and resource on which the decision applies and an eHealth platform reference number for tracing.

Example: SAML 2.0 Response with StatusCode'Deny'

```
< saml2p:Response... xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:Issuer>http://idp.smals-mvm.be/shibboleth</saml2:Issuer>
<saml2p:Status>
<saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
<saml2p:StatusCode Value="urn:be:fgov:health:1.0:status:xacml:decision:Deny"/>
</saml2p:StatusCode>
<saml2p:StatusMessage>User is not authorized to access requested
resource</saml2p:StatusMessage>
<saml2p:StatusDetail>
<XACMLAuthzDecisionStatement xmlns="urn:oasis:xacml:2.0:saml:assertion:schema:os"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
<xacml-context:Response>
<xacml-context:Result>
<xacml-context:Decision>Deny</xacml-context:Decision>
</xacml-context:Result>
</xacml-context:Response>
<xacml-context:Request>
<xacml-context:Subject>
<xacml-context:Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">
<xacml-context:AttributeValue>1356fef9d-607d-494d-aff1-37061aae89f4</xacml-
context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Subject>
<xacml-context:Resource>
<xacml-context:Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">
<xacml-context:AttributeValue>urn:health:test:sso</xacml- context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Resource>
<xacml-context:Action/>
<xacml-context:Environment>
<xacml-context:Attribute
AttributeId="urn:be:fgov:health:1.0:health-ref"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">
<xacml-context:AttributeValue>IDP00000ATNWX</xacml-context:AttributeValue>
</ saml2p:Response>
```

⁹ Only for SAML 2.0 Profiles

¹⁰ <http://docs.oasis-open.org/xacml/3.0/xacml-profile-saml2.0-v2-spec-en.pdf>



HTTP 403 Forbidden page

Not available for SSO Profiles that include an AttributeQuery call back.

Instead of returning a response to the SP, the eHealth IDP blocks access for the user by showing a friendly 403 Access Denied Error page at the end of the authentication/authorization process at the IDP.

This page includes the unique identifier for the current authentication session of the user in the eHealth IDP. He can use this information to contact the service desk if he does not agree with the decision.

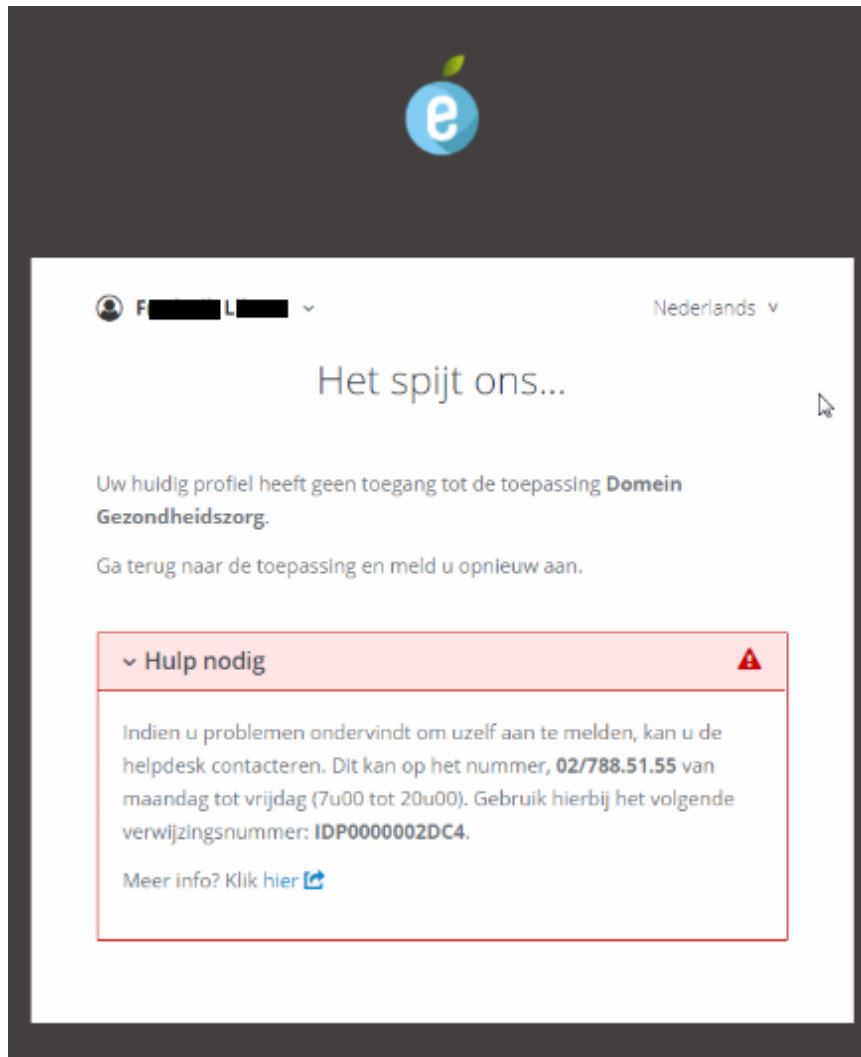


Figure 5: Access Denied error page (Dutch view)

5.2.5.4 Access denied by SP

When the publish-on-deny policy was other than the HTTP 403 page at the eHealth platform or if the deny decision is based on access rules executed by the SP, the SP MUST show the user a friendly message.

In case the decision is based on a 'Deny' from the eHealth platform, the SP MAY redirect the user to the NoAccess page of the eHealth IDP where the same standard friendly 'not authorized' message will be shown as if the publish-on- deny policy with the HTTP 403 page was used.

An SP/Application MAY also choose to show its own 'access denied' page if it feels that it is more appropriate for the target application. If done so, the SP/Application MUST display the '*urn:be:fgov:health:1.0:health-ref*' attribute on that page so the user is able to request help if he does not agree.

In ANY other case of access denial (which means Access Control Rules were executed by the SP), SPs MUST use an 'access denied' error page of their own. In this case, SPs SHOULD not use the



'urn:be:fgov:health:1.0:health-ref' attribute as the decision was made by additional access control rules, not by the eHealth platform. If a user disagrees, he should request help from the service desk of the SP.



6. Web Browser SSO Profiles

Most of the SSO profiles listed below are international standards for SSO with a Web Browser. Schemas and descriptions were taken from the official documentation, available in the internet:

- SAML 1.1 and 2.0: <http://saml.xml.org/saml-specifications>
- WS-Federation 1.2: <http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf>

6.1 SAML 2.0

The Web Browser SSO Profiles of the SAML 2.0 specifications define how to use SAML messages and bindings to support Web Single Sign-On. They provide a variety of options, primarily having to do with two dimensions of choice:

- First: whether the message flows are IDP-initiated or SP-initiated, and
- Second: which bindings are used to deliver messages between the IDP and the SP.

The first choice has to do with where the user starts the process of a web SSO exchange. SAML 2.0 supports two general message flows.

- The most common scenario for starting a web SSO exchange is the SP-initiated web SSO model which begins with the user choosing a browser bookmark or clicking a link that takes him directly to an SP application resource he wants to access. However, since the SP does not yet know the user, the SP sends the user to an IDP to authenticate before access is allowed to the resource. The IDP builds an assertion representing the user's authentication at the IDP and then sends the user back to the SP with the assertion. The SP processes the assertion and determines whether to grant the user access to the resource.
- The IDP-Initiated web SSO model is not supported by the IDP. It always expects an authentication request coming from the SP after a user tried to access a protected resource.

The second choice is to be made when using the SAML profiles centers around which SAML bindings will be used when sending messages back and forth between the IDP and SP. Many combinations of message flows and bindings are possible in SAML 2.0.

The ones supported by the eHealth IDP are listed below.

For the web SSO profile, communication consists mainly out of two SAML messages; namely, an Authentication Request message sent from an SP to an IDP, and a response message containing a SAML assertion that is sent from the IDP to the SP (and then, secondarily, with messages related to artifact resolution if that binding is chosen).

6.1.1 HTTP POST

In this profile, the SP delivers a SAML <AuthnRequest> message (through binding *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST* or *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect*¹¹ to the IDP and the binding *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST* is used to return the SAML <Response> message containing the assertion to the SP.

¹¹ The HTTP POST binding may be necessary for an <AuthnRequest> message in cases where its length precludes the use of the HTTP Redirect binding (which is typical). The message may be long enough to require a POST binding when, for example, it includes many of its optional elements and attributes, or when it must be digitally signed.

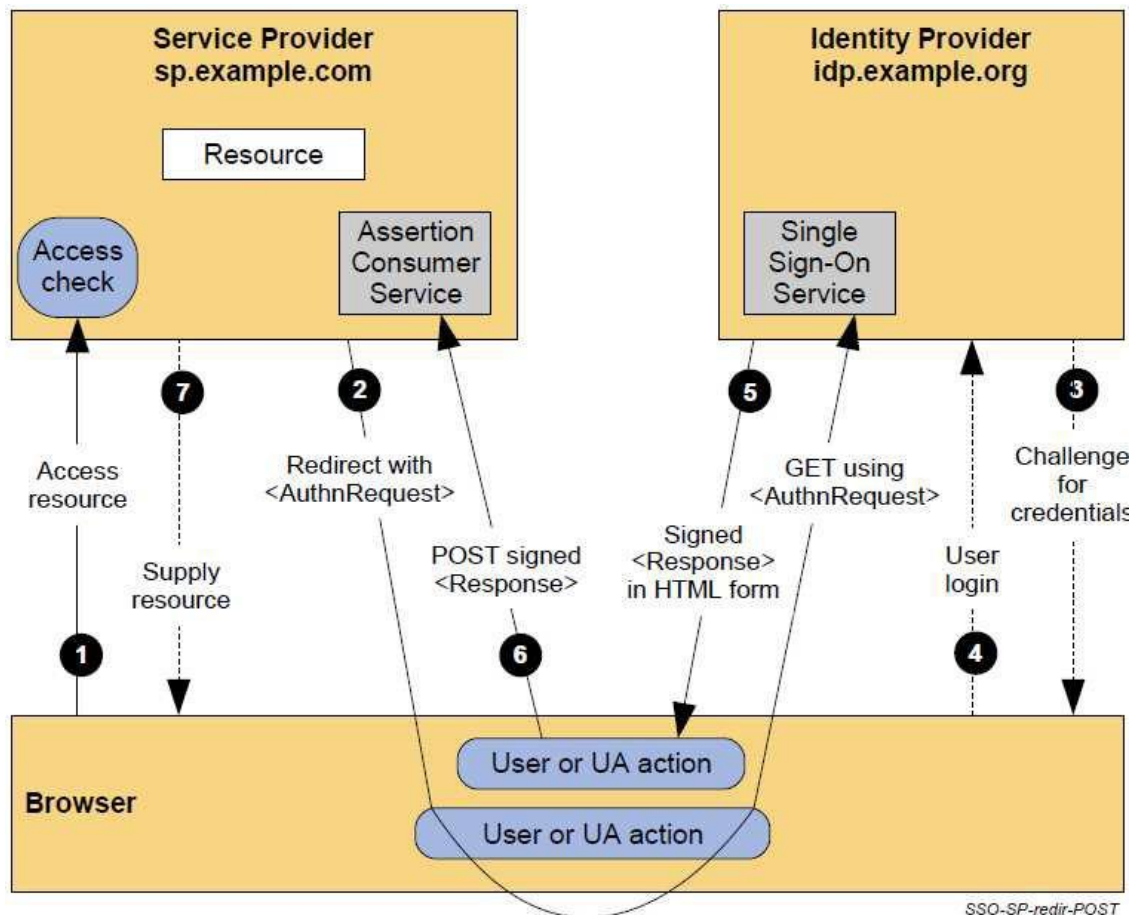


Figure 6: SAML 2.0 HTTP POST

1. The user attempts to access a resource on the SP. The user does not have a valid logon session (i.e. security context) on this site. The SP saves the requested resource URL in local state information that can be saved across the web SSO exchange.
2. The SP sends an HTTP redirect response to the browser (HTTP status 302 or 303). The Location HTTP header contains the destination URI of the Sign-On Service at the identity provider together with an <AuthnRequest> message encoded as a URL query variable named SAMLRequest. The browser processes the redirect response and issues an HTTP GET request to the IdP's Single Sign-On Service with the SAMLRequest query parameter. The local state information (or a reference to it) is also included in the HTTP response encoded in a RelayState query string parameter.

<https://www.ehealth.fgov.be/idp/profile/SAML2/SSO/Redirect?SAMLRequest=request&RelayState=token>

3. The SSO Service determines whether the user has an existing logon security context at the identity provider, meeting the default or requested (in the <AuthnRequest>) authentication policy requirements. If not, the IDP interacts with the browser to challenge the user to provide valid credentials.
4. The user provides valid credentials and a local logon security context is created for the user at the IDP.
5. The IDP SSO Service builds a SAML assertion representing the user's logon security context. Since a POST binding is going to be used, the assertion is digitally signed and then placed within a SAML <Response> message. The <Response> message is then placed within an HTML FORM as a hidden form control named SAMLResponse. If the IDP received a RelayState value from the SP, it must return it unmodified to the SP in a hidden form control named RelayState. The SSO Service sends the HTML form back to the browser in the HTTP response. For ease of use purposes, the HTML FORM will be accompanied by script code that will automatically post the form to the destination site.


```

<form method="post" action="https://sp.partner.be/SAML2/SSO/POST" ...>
  <input type="hidden" name="SAMLResponse" value="response" />
  <input type="hidden" name="RelayState" value="token" />
  ...
  <input type="submit" value="Submit" />
</form>

```

The value of the SAMLResponse parameter is the base64 encoding of the <samlp:Response> element, generated by the IDP.

6. The browser, due either to a user action or execution of an “auto-submit” script, issues an HTTP POST request to send the form to the SP's Assertion Consumer Service.

```

POST /SAML2/SSO/POST HTTP/1.1
Host: sp.partner.be
Content-Type: application/x-www-form-urlencoded
Content-Length: nnn
SAMLResponse=response&RelayState=token

```

where the values of the SAMLResponse and RelayState parameters are taken from the HTML form in Step 5. The SP's Assertion Consumer Service obtains the <Response> message from the HTML FORM for processing. The digital signature on the SAML assertion must first be validated and then the assertion contents are processed in order to create a local logon security context for the user at the SP. Once this completes, the SP retrieves the local state information indicated by the RelayState data to recall the originally-requested resource URL. It then sends an HTTP redirect response to the browser directing it to access the originally requested resource (not shown).

7. An access check is made to establish whether the user has the correct authorization to access the resource. If the access check passes, the resource is then returned to the browser.

6.1.2 HTTP-POST pull

The eHealth IDP supports also a variant on the SAML 2.0 HTTP-POST Profile where the SAML <Response> in step 5 of the schema above does not contain an AttributeStatement with the list of Identity and Authorization Attributes expected by the SP. Instead it only contains an AuthenticationStatement with a persistent identifier, generated by the IDP.

Once the SP is in possession of the identifier, it contacts the IDP's AttributeService using the synchronous urn:oasis:names:tc:SAML:2.0:bindings:SOAP binding to obtain ('pull') the SAML AttributeStatement that corresponds to the persistent identifier. This additional SP-IDP communications follows the Assertion Query/Request Profile.

The decision not to include the AttributeStatement in the POSTed form is made by the IDP and can be configured for any SP that wishes to use this variant of the profile. However, it cannot be altered per request. It will be activated for all or none of the authentication requests made by that particular SP.



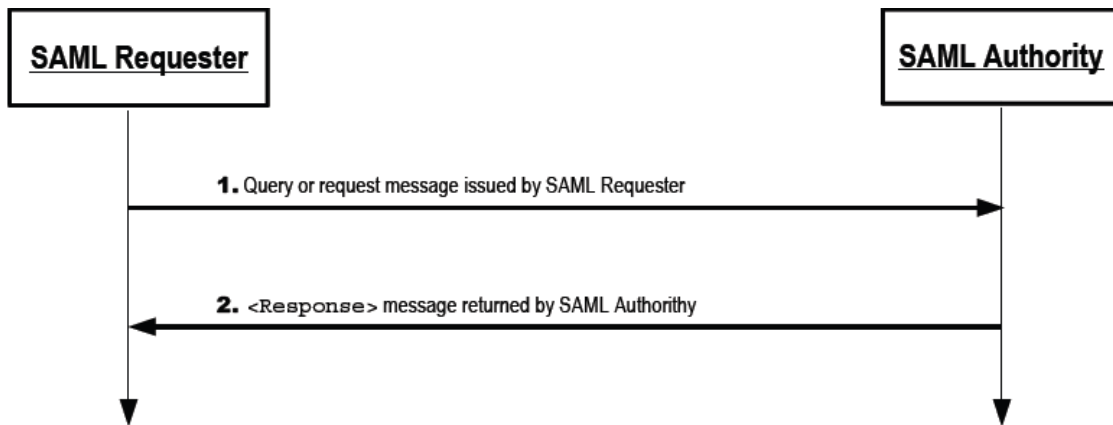


Figure 7: Assertion Query/Request Profile

1. The SP, acting as SAML Requester, initiates the profile by sending an <AttributeQuery> message to the IDP, acting as SAML authority.
2. The responding IDP (after processing the query) issues a <Response> message to the SP.

6.1.3 HTTP-Artifact

In this profile, the SP delivers a SAML <AuthnRequest> message (through binding `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST` or `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`¹¹) to the IDP and the SAML <Response> message is returned using the `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact` binding.

When using the HTTP Artifact binding for the SAML <Response> message, SAML permits the artifact to be delivered via the browser using either an HTTP POST or HTTP Redirect response (not to be confused with the SAML HTTP POST and Redirect Bindings).

Once the SP is in possession of the artifact, it contacts the IDP's Artifact Resolution Service using the synchronous 'urn:oasis:names:tc:SAML:2.0:bindings:SOAP' binding to obtain the SAML message that corresponds to the artifact.

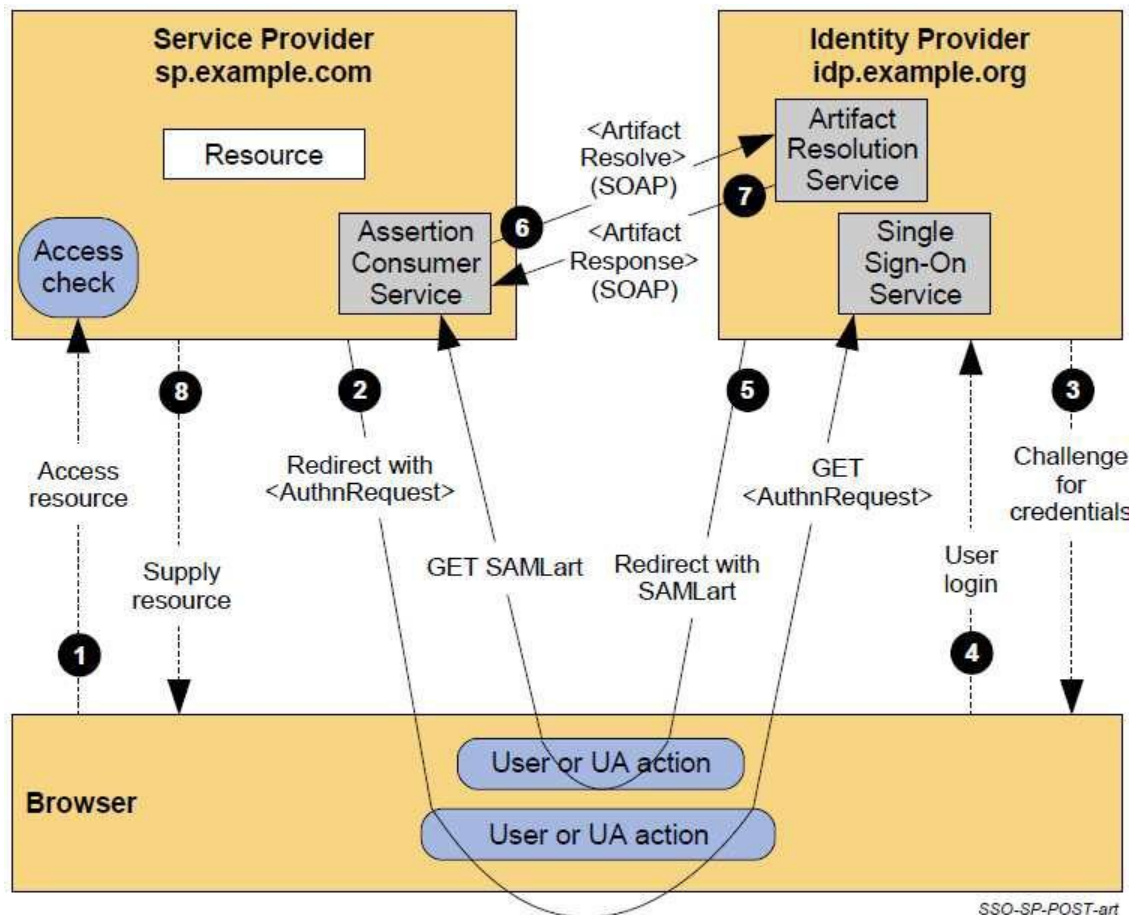


Figure 8: SAML 2.0 HTTP-Artifact

1. The user attempts to access a resource on sp.example.com. The user does not have a valid logon session (i.e. security context) on this site. The SP saves the requested resource URL in local state information that can be saved across the web SSO exchange.
2. The SP sends an HTML form back to the browser in the HTTP response (HTTP status 200). The HTML FORM contains a SAML <AuthnRequest> message encoded as the value of a hidden form control named SAMLRequest.

```
<form method="post" action="https://idp.ehealth.fgov.be/idp/profile/SAML2/SSO/POST" ...>
  <input type="hidden" name="SAMLRequest" value="request" />
  <input type="hidden" name="RelayState" value="token" />
  ...
  <input type="submit" value="Submit" />
</form>
```

The RelayState token is an opaque reference to state information maintained at the SP. The value of the SAMLRequest parameter is the base64 encoding of the <AuthnRequest> element, generated by the SP. For ease-of-use purposes, the HTML FORM typically will be accompanied by script code that will automatically post the form to the destination site (which is the IDP in this case). The browser, due either to a user action or execution of an “auto-submit” script, issues an HTTP POST request to send the form to the identity provider's Single Sign-On Service.

```
POST /idp/profile/SAML2/SSO/POST HTTP/1.1
Host: www.ehealth.fgov.be
Content-Type: application/x-www-form-urlencoded
```



Content-Length: nnn

SAMLRequest=request&RelayState=token

3. The Single Sign-On Service determines whether the user has an existing logon security context at the identity provider that meets the default or requested authentication policy requirements. If not, the IdP interacts with the browser to challenge the user to provide valid credentials.
4. The user provides valid credentials and a local logon security context is created for the user at the Id.
5. The IDP Single Sign-On Service issues a SAML assertion representing the user's logon security context and places the assertion within a SAML <Response> message. Since the HTTP Artifact binding will be used to deliver the SAML Response message, it is not mandated that the assertion be digitally signed. The IDP creates an artifact containing the source ID for the IDP site and a reference to the <Response> message (the MessageHandle). The HTTP Artifact binding allows the choice of either HTTP redirection or an HTML form POST as the mechanism to deliver the artifact to the partner. The figure shows the use of redirection.
6. The SP's Assertion Consumer Service now sends a SAML <ArtifactResolve> message containing the artifact to the IDP's Artifact Resolution Service endpoint. This exchange is performed using a synchronous SOAP message exchange containing an <ArtifactResolve> element.
7. The IDP's Artifact Resolution Service extracts the MessageHandle from the artifact and locates the original SAML <Response> message associated with it. This message is then placed inside a SAML <ArtifactResponse> message, which is returned to the SP over the SOAP channel. The SP extracts and processes the <Response> message and then processes the embedded assertion in order to create a local logon security context for the user at the SP. Once this is completed, the SP retrieves the local state information indicated by the RelayState data to recall the originally-requested resource URL. It then sends an HTTP redirect response to the browser directing it to access the originally requested resource (not shown).
8. An access check is made to establish whether the user has the correct authorization to access the resource. If the access check passes, the resource is then returned to the browser.

6.1.4 urn:mace:shibboleth:2.0:profiles:AuthnRequest

The profiles HTTP-POST and HTTP-Artifact listed in previous sections use in- and outbound bindings as described in the official specification.

The eHealth IDP also supports a variant on this where the inbound binding is different (= the binding for the AuthnRequest message from SP to IDP).

In this binding, registered as 'urn:mace:shibboleth:2.0:profiles:AuthnRequest', the AuthnRequest is not an xml message constructed by the SP but a simple GET to the location of the IDP that supports this binding. While constructing this URL, the following request parameters must be added by the SP before the message is redirected to the IDP:

- providerId: the unique identifier of the SP in the eHealth I.AM Federation
- shire: the location to which the IDP must send the SAML 2.0 Response (= AssertionConsumerService Location)
- target: a variable used to reference the target application at the SP.
- time: current time in milliseconds to prevent browser caching and replay attacks

This is in fact the same binding as is used in the eHealth IDP for the SAML 1.1 inbound bindings (since SAML 1.1 does not specify SP-Initiated SSO).

This binding is also by default supported by SPs using Shibboleth¹² software.

SPs that for some reason cannot use the official SAML 2.0 inbound bindings may choose to use this inbound binding instead.

6.2 SAML 1.1

The SAML 1.1 specifications define 2 Web SSO profiles. These profiles assume:



- Use of a standard commercial web browser using either HTTP or HTTPS.
- The user has authenticated to the local source site¹³
- The assertion's subject refers implicitly to the user that has been authenticated

Other than in SAML 2.0, the SAML 1.1 Web SSO Profiles only handle IDP-Initiated SSO. They do not specify how to solve SP-Initiated SSO:

What if a user tries to access directly the protected resource at the SP?

urn:mace:shibboleth:1.0:profiles:AuthnRequest

To solve this use case, the eHealth IDP supports an inbound binding for SP-Initiated SSO as published by the Shibboleth¹⁴ consortium in their implementation of the SAML 1.1 Web SSO profiles.

All SPs using Shibboleth Software will support this inbound binding by default.

Other SPs that wish/need to use a SAML 1.1 profile for communication with the eHealth IDP should implement it.

It is registered as binding “urn:mace:shibboleth:1.0:profiles:AuthnRequest”.

It comes down to the construction of one GET to start the initial communication with the IDP:

If a user tries to access a protected resource at the SP but he is not yet authenticated, the SP must redirect the user to the eHealth IDP SingleSignOnService Location that supports this binding (as published online in the SAML 2.0 Metadata of the IDP¹⁵) using an HTTP GET.

The following request parameters must be added to the location (location?request-parameters):

- providerId: the unique identifier of the SP in the eHealth I.AM Federation
- shire: the location to which the IDP must send the SAML 1.1 Response (= AssertionConsumerServiceLocation)
- target: a variable used to reference the target application at the SP.
- time: current time in milliseconds to prevent browser caching and replay attacks



6.2.1 Browser/POST

This represents a “push model”. An assertion is POSTed using the binding ‘urn:oasis:names:tc:SAML:1.0:profiles:browser-post’ directly to the relying party

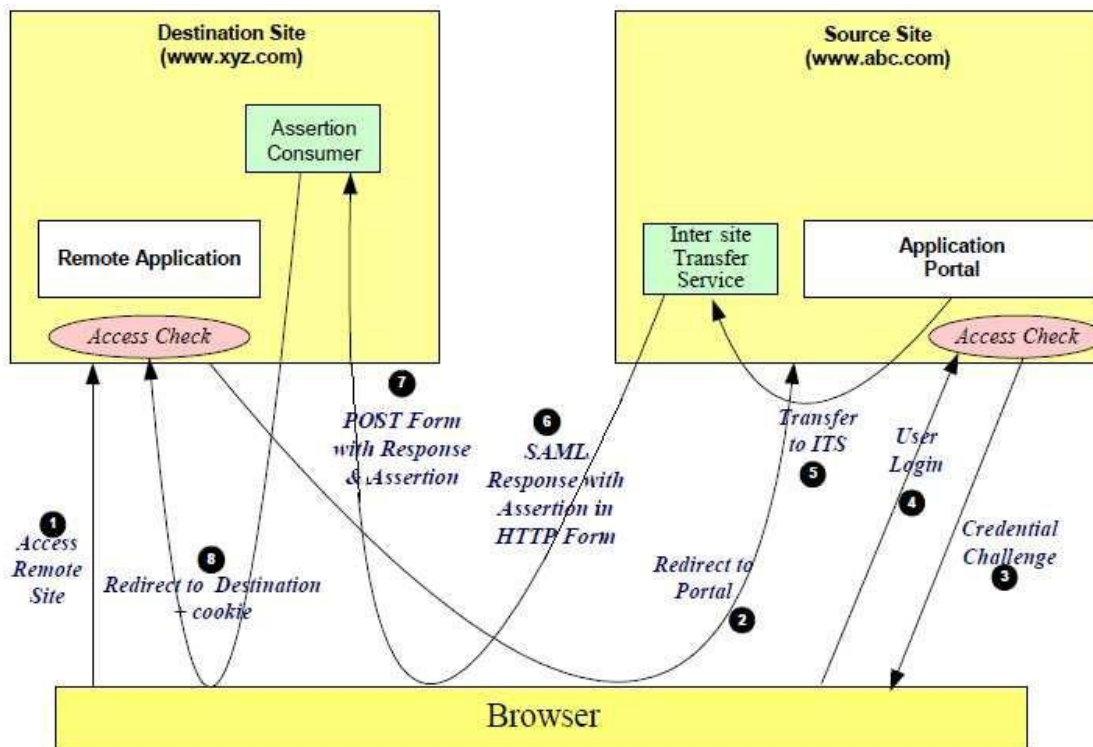


Figure 9: SAML 1.1 Browser/POST

1. The user accesses the destination web site (protected by the SP).
2. The destination web site performs an access check and determines that the user must be authenticated by the IDP (source site). A redirection is issued to the IDP source site. SAML 1.1 does not specify any details for this request. However, as described at the start of the SAML 1.1 Web SSO Profiles section, the GET redirect must point to a SingleSignOnService location of the IDP supporting the binding ‘urn:mace:shibboleth:1.0:profiles:AuthnRequest’ and contain a few request parameters.
3. The source site (the asserting party) challenges the user for their credentials.
4. The user supplies back credentials, for instance eID, token Fedict.
5. Internal redirect in the eHealth IDP.
6. The IDP sends a HTML form back to the browser. The HTML FORM contains a SAML response, within which is a SAML assertion. The SAML specifications mandate that the response must be digitally signed. Typically the HTML FORM will contain an input or submit action that will result in a HTTP POST.
7. The browser, either due to a user action or via an “auto-submit”, issues a HTTP POST containing the SAML response to be sent to the destination’s (relying party) Assertion Consumer service.
8. The replying party’s Assertion Consumer validates the digital signature on the SAML Response. If this validates, it sends a redirection message containing a cookie back to the browser. The cookie identifies the session. The Browser then processes the redirect message and issues a HTTP GET to the TARGET resource at the SP originally requested in step 1.

6.2.2 Browser/POST pull

The eHealth IDP supports also a variant on the SAML 1.1 Browser/POST Profile where the SAML <Response> in step 6 of the schema above does not contain an AttributeStatement with the list of Identity and Authorization Attributes expected by the SP. Instead, it only contains an AuthenticationStatement with a persistent identifier, generated by the IDP.

Once the SP is in possession of the identifier, it contacts the IDP's AttributeService using the synchronous 'urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding' binding to obtain the SAML AttributeStatement that corresponds to the persistent identifier.

This profile might be more appropriate than the standard SAML 1.1 Browser/POST push model since SAML 1.1 does not support encryption. The <Response> message from IDP to SP is sent using the browser of the user and all transferred data will be visible for him. In some cases, this may cause privacy issues.

The decision not to include the AttributeStatement in the POSTed form is made by the IDP and can be configured for any SP that wishes or needs to use this variant of the profile. However, it cannot be altered per request. It will be activated for all or none of the authentication requests made by that particular SP.

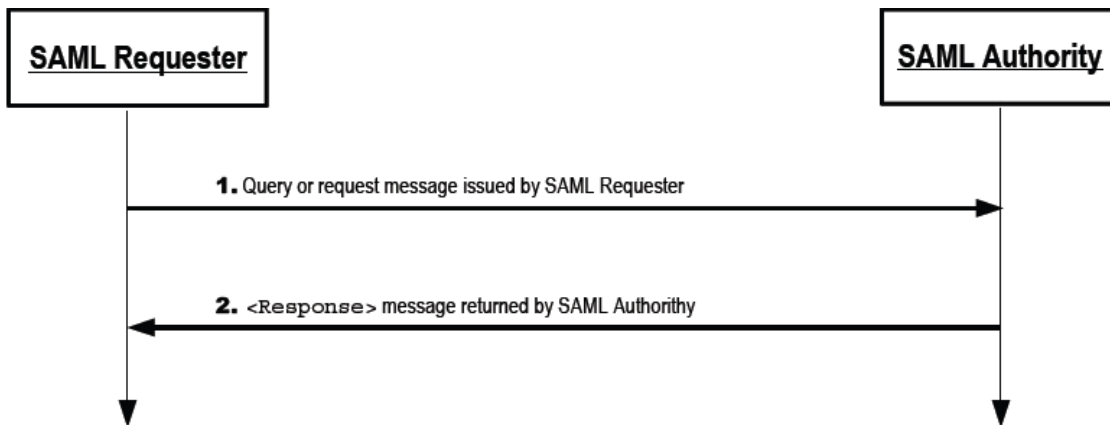


Figure 10: Assertion Query/Request Profile

1. The SP, acting as SAML Requester, initiates the profile by sending a <Request> containing an <AttributeQuery> message to the IDP, acting as SAML authority.
2. The responding IDP (after processing the query) issues a <Response> message to the SP.

6.2.3 Browser/Artifact

This represents a “pull model”. A special form of reference to the authentication assertion (called an artifact) is sent to the relying party using the binding ‘urn:oasis:names:tc:SAML:1.0:profiles:artifact-01’, which can use this reference to obtain (or pull) the assertion from the Asserting Party using the ‘urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding’ binding.

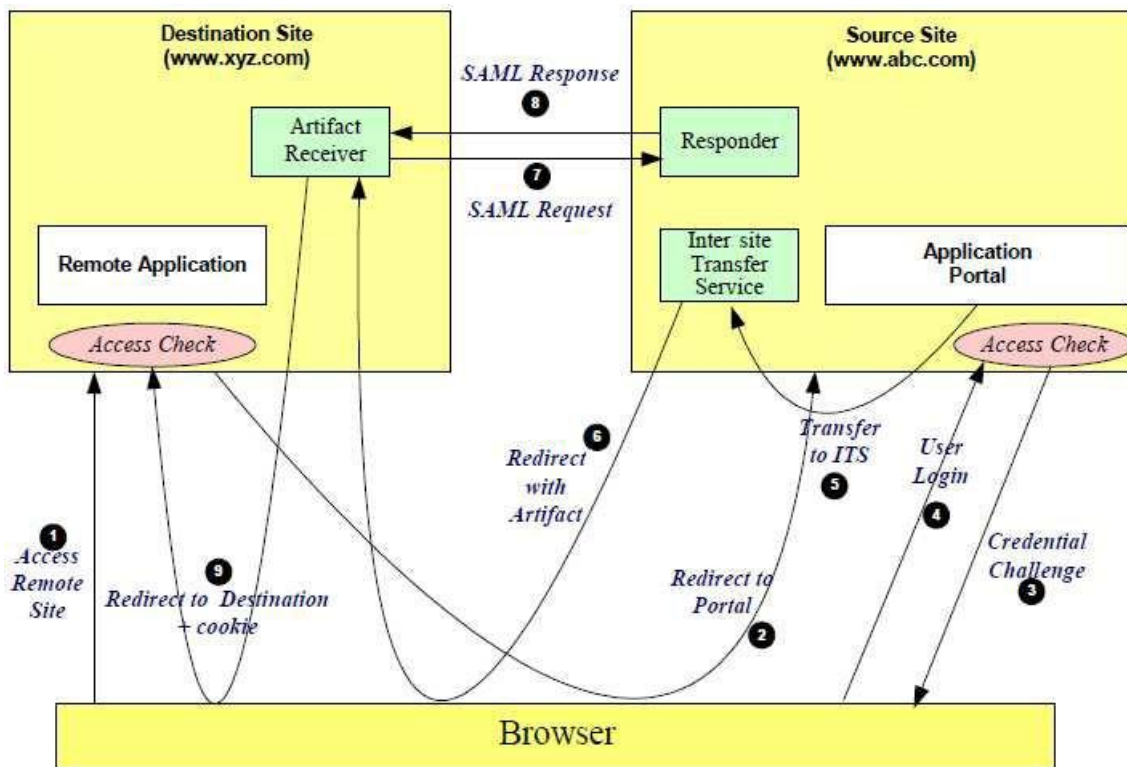


Figure 11: SAML 1.1 Browser/Artifact

1. The user accesses the destination web site (protected by the SP).
2. The destination web site performs an access check and determines that the user must be authenticated by the IDP (source site). A redirection is issued to the IDP source site. SAML 1.1 does not specify any details for this request. However, as described at the start of the SAML 1.1 Web SSO Profiles section, the GET redirect must point to an SSO Service location of the IDP supporting the binding ‘urn:mace:shibboleth:1.0:profiles:AuthnRequest’ and contain a few request parameters.
3. The source site (the asserting party) challenges the user for their credentials.
4. The user supplies back credentials, for instance eID, token Fedict.
5. Internal redirect in the eHealth IDP.
6. The IDP generates an assertion for the user while also creating an artifact. The artifact contains the source ID of the IDP SAML responder together with a reference to the assertion (the AssertionHandle). The IDP then sends back an HTTP redirection response to the browser, with the HTTP location header containing the URL of the Artifact Receiver service, the TARGET URL, and the artifact.
7. On receiving the HTTP message, the Artifact Receiver on the destination site sends a SAML request to the IDP SAML responder containing the artifact supplied by the IDP.
8. The IDP SAML responder supplies back a SAML response message containing the assertion generated during step 7.
9. The Artifact Receiver, on the destination web site, sends a redirection message containing a cookie back to the browser. The cookie identifies the session. The Browser then processes the redirect message and issues a HTTP GET to the TARGET resource at the SP originally requested in step 1.

7. Configuration options

The eHealth IDP Authentication Wizard consists of dynamic pages. For each application the wizard can behave somewhat differently according to configuration options set by eHealth in its Metadata or set by the SP when requesting authentication.

Configuration options set in eHealth Metadata are static (the same for each request to the application). Configuration options set by the SP can be per request.

7.1 Metadata@eHealth

On registration, a partner can specify some configuration options in the registration form¹⁸:

- Logo : on top of each page a logo is shown. By default, it is the healthcare logo.



- Footer help : if the SP wants to offer his own help page, he must publish its own page and provide the URL.
- ServiceName: name of the application as it is shown on each wizard page during authentication.
- Languages: languages (nl, fr, de) that should be supported in the wizard. Users requesting authentication for applications that are for one language only will not be prompted to choose a language.
- Minimum authentication level: Minimum authentication level used to propose authentication methods to the user may choose from (methods within a lower authentication level than demanded in the DU, will never be shown).
- ForceAuthn: if true, users will be forced to authenticate at the IDP for each request by the SP for this application, even if they were already authenticated during their active browser session (this breaks SSO).
- ProfileOptions: type of profiles applicable for the application. eHealth will not search for other type of profiles upon authentication of users for that particular application.
- IsPassive: if true, eHealth will limit the user interface and interaction with the user during his authentication request.
 - o If only one supported authentication method is applicable, it will be automatically chosen (step 2 of the wizard is skipped).
 - o If the user only has the profile of type 'citizen' available, and the application is available for profile type 'citizen', this profile type will be automatically chosen (step 3 of the wizard is skipped). This only happens if the application asked for an active load of the list of children of the user (this means that the attribute "lazyLoadChildren" is set to false in eHealth's metadata).
- Certified Attributes: Basic authentication attributes which together form the identity of the user are sent by default. Additional certified attributes can be requested by the application on behalf of the authenticated user. These can be configured in eHealth's Metadata for each registered application.



7.2 SP AuthnRequest

The options configured in Metadata@eHealth are static and the same for each request of the SP for one specific application.

If an SP needs dynamic configuration, on a per-request basis, some of the options can be overridden by adding them to the authentication request.

7.2.1 HTTP Request Parameters

Languages: If an application is registered with support for more than 1 language but a language was already chosen at the partner site, the chosen language can be passed to the SingleSignOnService Location of the IDP as an extra request parameter 'language', value 'nl' (Dutch) or 'fr' (French) or 'de' (German)..

7.2.2 SAML 2.0 AuthRequest

If you are using one of the SAML 2.0 Profiles, which sends a SAML 2.0 AuthnRequest to the eHealth IDP, you can add specific attributes and elements to it to override some configuration options.

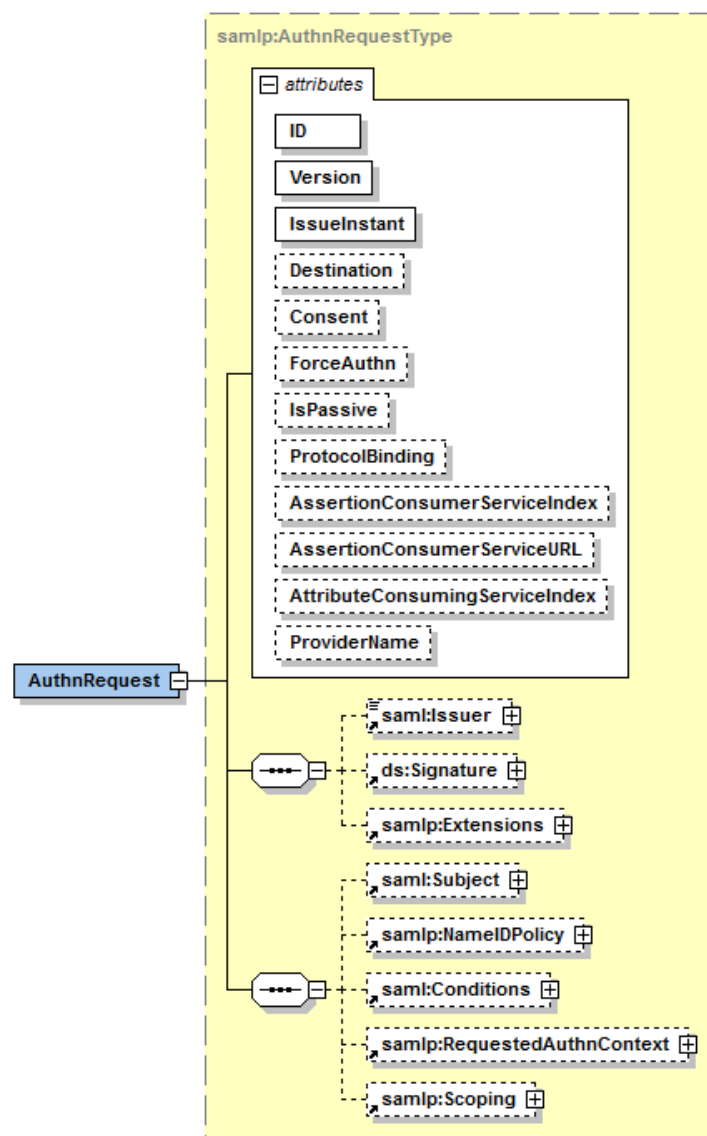


Figure 13: SAML 2.0 AuthnRequest

- ForceAuthn: overrides decision set by default in Metadata@eHealth

- IsPassive: overrides decision set by default in Metadata@eHealth
- AttributeConsumingServiceIndex: by default, eHealth uses the AssertionConsumerServiceURL to decide for which application the authentication request is meant. If this distinction cannot be made based on that URL, you can specify this field. The index MUST be configured in Metadata@eHealth for the calling SP.
- <RequestedAuthnContext>: to specify a subset of the applicable AuthenticationMethods for the requested application.
 - Comparison: exact (default), minimum, maximum, better
 - <AuthnContextClassRef>: one or more AuthnContextClassRefs supported by eHealth (each supported AuthnContextClassRef is linked to one AuthenticationMethod and is registered with a security level which will be used in the comparison for minimum, maximum, better (if applicable). AuthnContextClassRef elements that violate the security level of the application, as registered at eHealth, will be ignored.
- <Extensions>: extendable point in the SAML Specs to allow for configuration out of scope of SAML 2.0.
- Languages: to specify a chosen language, following SAML 2.0 Attribute can be placed in the <Extensions> element where 'xx' is 'nl' (Dutch) or 'fr' (French) or 'de' (German). Other languages will be ignored.


```

0      <saml:Attribute Name="PrefLanguage" NameFormat="
urn:oasis:names:tc:SAML:2.0:profiles:attribute:basic"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">xx</saml:AttributeValue></saml:Attribute>

```



8. Risks and security

8.1 Risks & safety

8.1.1 Web SSO

8.1.1.1 AuthnRequest

Web SSO Authentication Requests from a requesting SP to eHealth are sent over a one-way SSL connection.

Depending on the used SSO Profile (see 'eHealth I.AM - IDP'), the request from an SP can include an enveloped signature as described in the SAML Specifications (1.x or 2.0).

This signature will be used to authenticate the SP as requesting entity.

The key used to sign these messages must be stored on the partner system in a secure manner in order to prevent unauthorized use.

8.1.1.2 Response

In response to a Web SSO AuthnRequest, eHealth will send a signed Response.

The recipient should process the Response following the processing rules as described in the specifications of the used SSO Profile (see 'eHealth I.AM - IDP').

The recipient (SP) must also verify if the Response is signed by a valid eHealth IDP certificate and that it is untampered with.

The eHealth IDP certificates are published online using SAML 2.0 Metadata (See eHealth I.AM – Federation Metadata for more information). If the used SSO Profile is SAML 2.0 HTTP-POST, the response from eHealth will also be encrypted with a certificate belonging to the recipient (SP).

8.2 Security

8.2.1 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.



9. Test and release procedure

9.1 Procedure

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

9.1.1 Initiation

If you intend to use the eHealth platform service, please contact info@ehealth.fgov.be. The project department will provide you with the necessary information and mandatory documents.

9.1.2 Development and test procedure

You have to develop/configure your SP in order to connect to our IAM IDP.

Most of the info required for integration is published on the portal of the eHealth platform.

Before using IAM IDP in any environment, your project may have been approved by the eHealth platform (see Initiation step).

When the project is considered as ready, you have to provide all useful information (such technical specification from your SP, test users information, ...) to your point of contact at the eHealth platform.

eHealth platform will then prepare the environment and warn you when the setup is ready. From this moment, you start the integration and acceptance tests. The eHealth platform suggests testing during minimum one month.

After successful acceptance tests, the partner sends his test results (and eventually performance results) by email to his point of contact at the eHealth platform.

Then the eHealth platform and the partner agree on a release date. The eHealth platform prepares the connection to the production environment (with necessary information provided by the partner).

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.

9.1.3 Operational follow-up

Once in production, the partner using the eHealth platform service for one of his 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.



10. Error and failure messages

eHealth I.AM IDP may expose some alert / warning or error messages. Here are some examples :

10.1 Info



10.2 Warning



10.3 Errors

Errors are shown in a separate view to inform the user that something went wrong and to instruct the user that he should restart authentication from the application he tried to access, if possible.

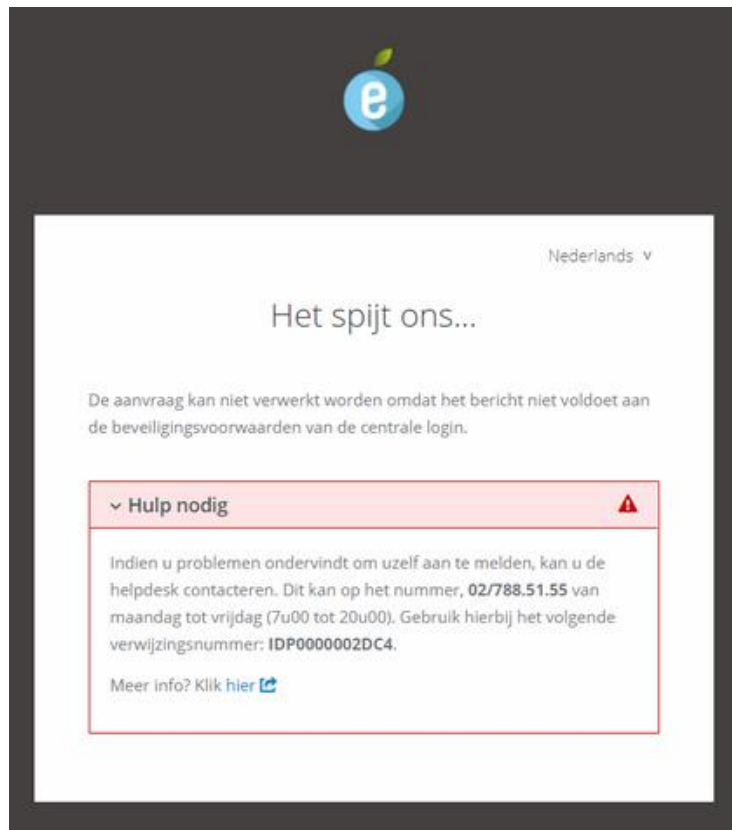
Some common error pages below (list not exhaustive).

10.3.1 Request rejected

The SP hosting the requested application is not configured properly to send requests to eHealth IDP.

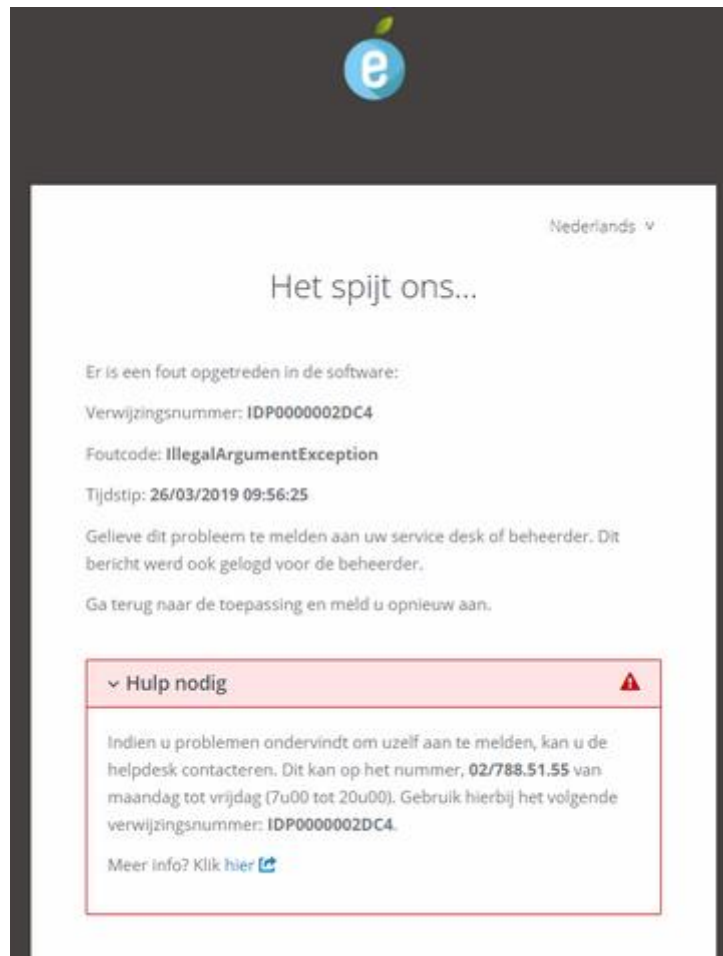
User should not retry.

Problem in configuration that needs to be fixed by the SP or by eHealth platform in IDP metadata.



10.3.2 Unexpected error

In case an unexpected error occurs for which no specific error mapping exists, a general error page is shown.



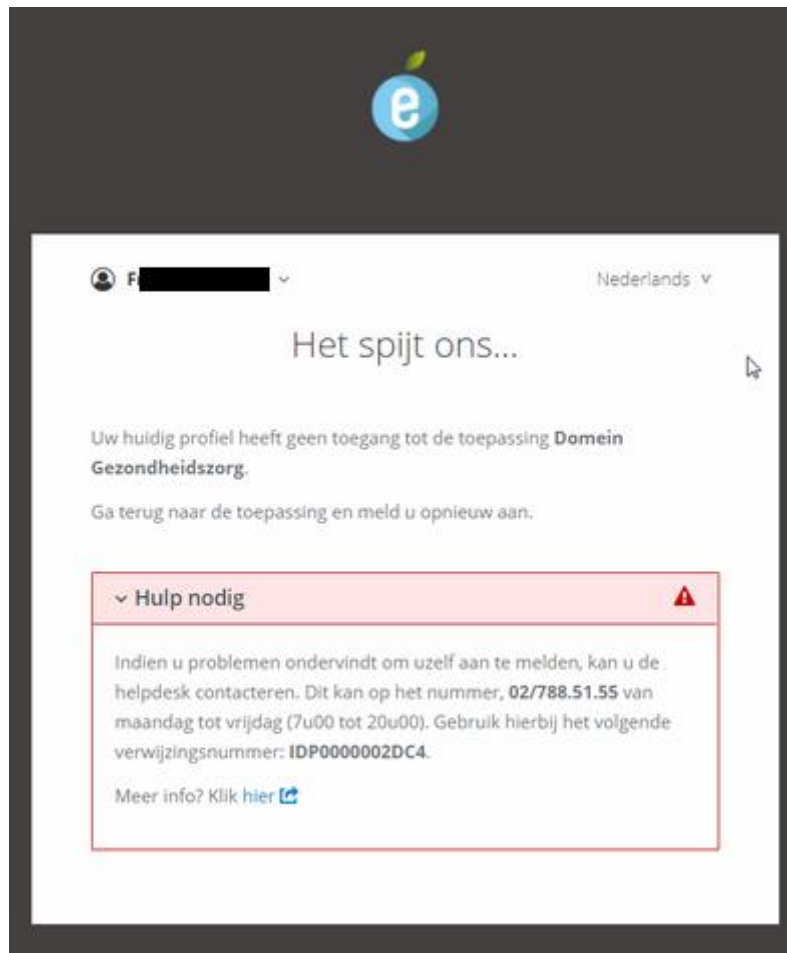
The screenshot shows a web page with a dark header containing a blue circle with a white 'e' and a green leaf. The main content area is white and features a language selector 'Nederlands' with a dropdown arrow. The heading 'Het spijt ons...' is centered. Below it, the text reads: 'Er is een fout opgetreden in de software: Verwijzingsnummer: IDP0000002DC4 Foutcode: IllegalArgumentException Tijdstip: 26/03/2019 09:56:25'. Further instructions state: 'Gelieve dit probleem te melden aan uw service desk of beheerder. Dit bericht werd ook gelogd voor de beheerder. Ga terug naar de toepassing en meld u opnieuw aan.' A red-bordered box titled 'Hulp nodig' with a warning triangle icon contains the text: 'Indien u problemen ondervindt om uzelf aan te melden, kan u de helpdesk contacteren. Dit kan op het nummer, 02/788.51.55 van maandag tot vrijdag (7u00 tot 20u00). Gebruik hierbij het volgende verwijzingsnummer: IDP0000002DC4. Meer info? Klik hier' with a blue link icon.

10.3.3 User errors

Errors that are caused by a 'wrong' action of the end-user are not really to be considered as errors from the point of view of the IDP. They show a page to the end-user and a help section to inform him.

10.3.3.1 NoAccess

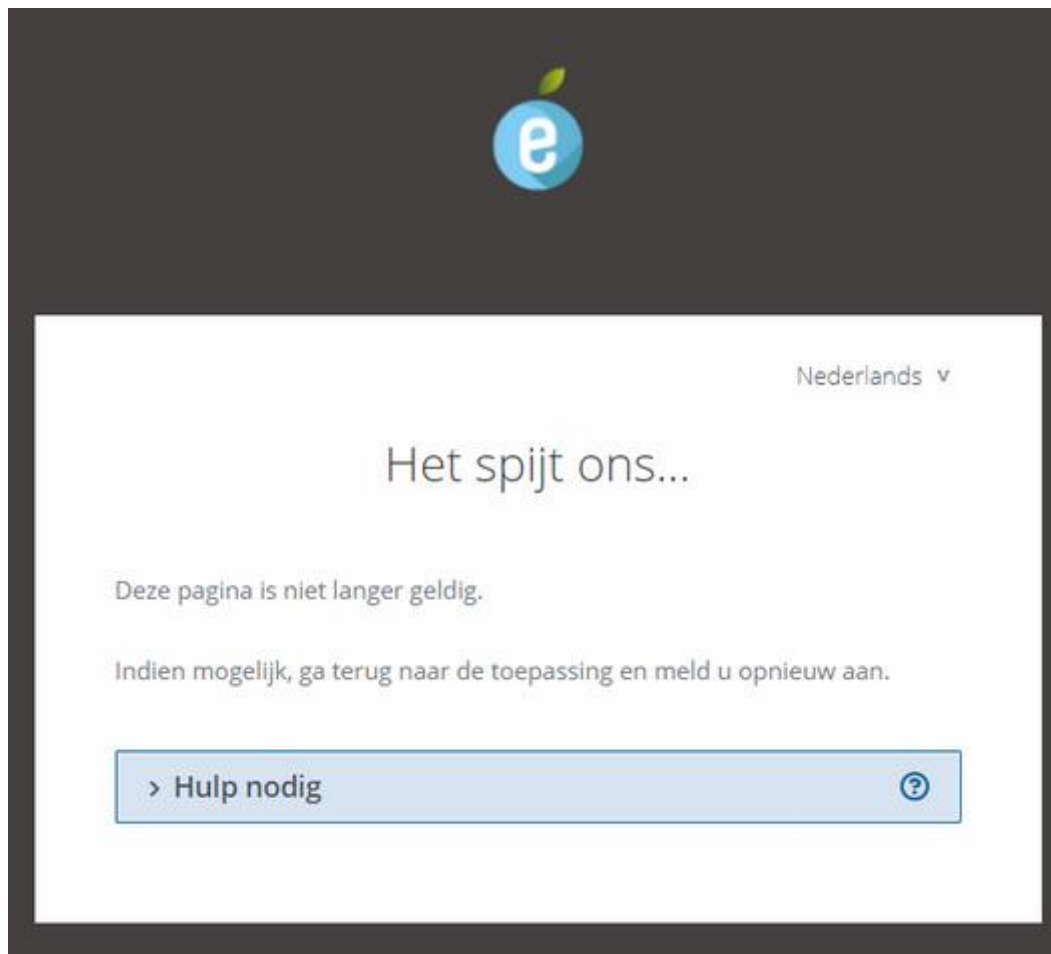
User does not have access to the requested application. He should use another profile (if possible) or refer to the contact center.



10.3.3.2 Step

User clicks the back button of the browser or uses a link that is no longer valid.

eHealth I.AM IDP does not keep history of SSO flows so it cannot replay previous actions. That would lead to an unpredictable outcome.



▼ Hulp nodig

U krijgt deze pagina te zien omdat u gebruik hebt gemaakt van de "Terug"-knop tijdens het surfen binnen de afgeschermdde toepassing. Het is ook mogelijk dat u de centrale login toegevoegd hebt aan uw favorieten/bookmarks in plaats van de toepassing zelf of u hebt een foute link van iemand ontvangen.

Indien u problemen ondervindt om uzelf aan te melden, kan u de helpdesk contacteren. Dit kan op het nummer, **02/788.51.55** van maandag tot vrijdag (7u00 tot 20u00). Gebruik hierbij het volgende verwijzingsnummer: **IDP0000002DC4**.

Meer info? Klik [hier](#) 



10.3.3.3 NotFound

User uses url that does not map to an SSO profile or other service.

