Identity & Authorization Management (I.AM) Registration - Joined IDP Protected Service

Environment :	**Integration** **Acceptation** **Production**

Contact	**:**	[*info@ehealth.fgov.be*](mailto:info@ehealth.fgov.be)
Pages	**:**	4

Summary

This document is made to be joined with a filled I.AM Registration form and aims to allow the Partner to describe one of his IDP Protected Service.

The form and it's Protected Services must be joined to the I.AM Registration form.

Version	Status	Date	Author	Description
1.0	Draft	12/12/18	eHealth platform	Initial version
1.1	Draft	10/08/20	eHealth platform	Revision
1.2	Final	20/01/21	eHealth platform	Final review, adapt contact info

Fill out the form to register the service at the eHealth IDP.

Identification	
Joined file [1]	
ContactPerson	
Name	
Email	
SP Authentication	
EntityID[2]	
AssertionConsumerService Location(s)[3]	i.e : https://XYZ/Shibboleth.sso/SAML2/POST (Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST")

[1] *In this field, you must indicate the name of the "I AM Registration form" linked to this IDP form*

[2] *Aka providerId, shire, issuer. Please use an URI or URL style ID*

[3] *URL on which the SP expects the response of the IDP. This must be unique for each application. You can define multiple URLs. Each URL must be linked with their binding (i.e*

https://XYZ/Shibboleth.sso/SAML2/POST (Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST")

X.509 Certificate for message signing[4]	
X.509 Certificate for message encryption[5]	
Authentication Wizard	
ServiceName (nl)	
ServiceName (fr)	
ServiceName (de)	

[4] *Base64 encoded format of the certificate used to sign messages to the Identity Services (for some IDP profiles there are no signed messages. If you are in such a situation and do not use any other identity service, you can leave the field blank).*

[5] *Base64 encoded format of the certificate used to encrypt messages to the partner (only a few profiles use encryption of messages. If you use a profile without encryption of messages, you can leave the field blank).*

Languages	nl fr de
Force Authentication[6]	
Profile Options	Citizen Parent Quality Organization Mandate
Is Passive[7]	
Authorization	
Publish-on-deny policy[8] **(please select only one)**	Attributes StatusCode 403 Forbidden Page eHealth

[6] *This will force users to re-authenticate for your application, even if they already were authenticated during their active browser session.*

[7] *IsPassive feature allows to automatically log in a user on a web page without any user interaction, under the condition that the logged in user profile is one of the user profiles allowed for this application*

[8] *On an authorization decision 'Deny', eHealth offers different options for the notification of this decision:*

- *Attributes: a SAML Token is returned with an AttributeStatement including the decision. An additional AuthzDecisionStatement can be added as well (see previous section).*
- *StatusCode: a SAML Status error is returned with a specific StatusCode.*
- *HTTP 403: the standard eHealth 'not authorized' errorpage is shown (no response is sent back to the SP)*