

Lasso - Bug #1309

has_synchronous_methods is designed when Authentic is IDP and not when Authentic is SP

13 mars 2012 16:59 - Arnaud Maillet

Statut:	Fermé	Début:	13 mars 2012
Priorité:	Normal	Echéance:	
Assigné à:		% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:	future	Planning:	
Patch proposé:			
Description			
Hello,			
Here is my configuration :			
SP : Authentic IDP : My server			
When the SP (Authentic) builds an Authnrequest (Single Sign On) for the IDP (my server) there is a call to :			
lasso_saml20_provider_get_first_http_method			
This method retrieves the supported binding "SingleSignOnService" of the IDP and checks that this one is synchronous :			
<pre>if (http_method_kind(result) == SYNCHRONOUS && ! has_synchronous_methods(provider, protocol_type)) continue;</pre>			
For example result = LASSO_HTTP_METHOD_REDIRECT and protocol_type = LASSO_MD_PROTOCOL_TYPE_SINGLE_SIGN_ON.			
If the retrieved method of the IDP is synchronous, this one also check that the provider (SP) has synchronous methods to retrieve the SAMLResponse of the IDP :			
<pre>if (http_method_kind(result) == SYNCHRONOUS && ! has_synchronous_methods(provider, protocol_type)) continue;</pre>			
The problem of "has_synchronous_methods" is :			
kind = profile_names[protocol_type]; // in our case : kind = "SingleSignOnService"			
<pre>if (endpoint_type && lasso_strisequal(endpoint_type->kind, kind)) { result = binding_uri_to_http_method(endpoint_type->binding); if (http_method_kind(result) == SYNCHRONOUS) return TRUE; }</pre>			
In this configuration, the SP doesn't have a "SingleSignOnService" kind because it's a SP :			
<pre><ns0:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://192.168.0.25:8000/authsaml2/singleLogout" ResponseLocation="http://192.168.0.25:8000/authsaml2/singleLogoutReturn"/> <ns0:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="http://192.168.0.25:8000/authsaml2/singleLogoutSOAP"/> <ns0:ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="http://192.168.0.25:8000/authsaml2/manageNameIdSOAP"/> <ns0:ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://192.168.0.25:8000/authsaml2/manageNameId" ResponseLocation="http://192.168.0.25:8000/authsaml2/manageNameIdReturn"/> <ns0:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="http://192.168.0.25:8000/authsaml2/singleSignOnArtifact" index="1"/></pre>			

```
<ns0:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://192.168.0.25:8000/authsaml2/singleSignOnPost" index="2"/>
```

I think in this function when the call is made by an SP, kind should be "AssertionConsumerService " :

```
kind = profile_names[protocol_type]; // should return AssertionConsumerService
```

Because we have to check that the SP can retrieve the SAMLResponse, and the kind to check is "AssertionConsumerService" and not "SingleSignOnService" when the provider is an SP.

What do you think about that?

Regards,

Historique

#1 - 17 mars 2012 13:58 - Benjamin Dauvergne

- Fichier *lasso_saml20_provider_get_first_http_method.diff* ajouté

Your analysis of the problem is good. I attach a patch to fix it. Could you verify that it really fixes your problem ??

#2 - 19 mars 2012 17:00 - Arnaud Maillet

The patch seems ok, I try with Authentic as an SP and Authentic as an IDP and I didn't find any problem.

#3 - 19 mars 2012 17:07 - Arnaud Maillet

hm I tried with Authentic as an SP and Authentic as an IDP and I didn't find any problem.

#4 - 03 septembre 2015 16:47 - Benjamin Dauvergne

- *Version cible mis à future*

#5 - 03 septembre 2015 17:06 - Benjamin Dauvergne

- *Statut changé de Nouveau à Fermé*

Published as part of the 2.3.6 release.

Fichiers

lasso_saml20_provider_get_first_http_method.diff

2,04 ko

17 mars 2012

Benjamin Dauvergne