Authentic 2 - Development #5540

Possibility to create saml service provider from its AssertionConsumerService endpoint

19 septembre 2014 10:08 - Frédéric Péters

Statut:	Nouveau		**Début:**	19 septembre 2014
Priorité:	Normal		**Echéance:**	
Assigné à:			**% réalisé:**	0%
Catégorie:			**Temps estimé:**	0:00 heure
Version cible:	2.2.0			
Patch proposed:	Non		**Planning:**	

Description

Dropbox doesn't distribute a saml metadata file, it just gives out its assertion consumer service endpoint (https://www.dropbox.com/saml_login); it would be useful to be able to create a service provider without having to forge a fake metadata file.

For refererence the simplesamlphp configuration amounts to:

```
$metadata['Dropbox'] = array (
        'AssertionConsumerService' => 'https://www.dropbox.com/saml_login',
        'simplesaml.attributes' => true,
        'simplesaml.nameidattribute' => 'mail',
        'NameIDFormat' => 'urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress',
);
```

Demandes liées:

Lié à Authentic 2 - Development #5541: Add a page to manage providers	**Fermé**	**19 septembre 2014**

Historique

#1 - 19 septembre 2014 10:19 - Benjamin Dauvergne

How does-it work without specifying the entity ID for dropbox ? Does ssp accept all AuthnRequest ? How does it find the ACS if the AuthnRequest does not containt its URL and it doesn't know the service entityID either ?

#2 - 19 septembre 2014 10:33 - Benjamin Dauvergne

I answer myself: I read the code for ssp and the dictionnary key is in fact the EntityID, so the configuration would be:

- EntityID, required
- ACS URL & method (POST [default] / Artifact), required
- LogoutServiceURL URL & method (Redirect [default] / SOAP), optional
- Certificate, optional

#3 - 19 septembre 2014 10:39 - Frédéric Péters

https://www.dropbox.com/help/1921#custom is the dropbox documentation.

You'll find some screenshots about salesforce configuration on https://developer.salesforce.com/page/Configuring-SAML-SSO-to-Dropbox (searching for "dropbox configuration saml" yields results for various other providers).

#4 - 08 octobre 2014 18:21 - Benjamin Dauvergne

- Statut changé de Nouveau à En cours

- Assigné à mis à Benjamin Dauvergne

How I see it:

- first add field to hold the metadata URL, to separate it from the entity ID
- remove special creation form for building from Metadata URL (the field will now be part of the model)
- make EntityID field editable, and required
- add new fields:
    - ACS URL, URLField, nullable, optional
    - ACS Method, CharField, choices, nullable, required if ACS URL is set
    - Logout URL, URLField, nullable, optional, forbidden if ACS URL is not set
    - Logout Method, CharField, choices, nullable, optional, required if Logout URL is set
- make the metadata field uneditable if ACS URL is not null, add text telling that to edit it all direct settings must be removed

- in LibertyProvider clean:
  - if metadata URL is set and metadata content or manual configuration field have changed, raise ValidationError telling that a web refresh must be done or the URL be removed,
  - if metadata and manual field have changed, raise ValidationError
  - if metadata has changed or object is new (no self.pk), clear all "manual" configuration fields, extract entityID from metadata
  - if entityID has changed but no other manual configuration field is set, raise ValidationError
  - if any manual configuration field has changed, clear metadata and generate new version from them
  - for all cases generate new entityID SHA1 hash (it's already done)

#5 - 20 novembre 2014 10:03 - Benjamin Dauvergne

- Statut changé de En cours à Nouveau

#6 - 06 mars 2015 15:28 - Benjamin Dauvergne

- Lié à Development #5541: Add a page to manage providers ajouté

#7 - 06 mars 2015 15:28 - Benjamin Dauvergne

- Priorité changé de Normal à Haut

#8 - 06 mars 2015 16:35 - Benjamin Dauvergne

- Version cible mis à future

#9 - 06 mars 2015 16:37 - Benjamin Dauvergne

- Version cible changé de future à 2.1.12

#10 - 17 mars 2015 16:59 - Benjamin Dauvergne

- Version cible changé de 2.1.12 à 2.1.13

#11 - 23 mars 2015 16:31 - Benjamin Dauvergne

- Version cible changé de 2.1.13 à 2.2.0

#12 - 11 mai 2015 11:06 - Benjamin Dauvergne

- Priorité changé de Haut à Normal

#13 - 10 mai 2016 16:38 - Mikaël Ates

- Tracker changé de Bug à Development

#14 - 12 janvier 2022 17:30 - Benjamin Dauvergne

- Assigné à Benjamin Dauvergne supprimé