pySAML2

Roland Hedberg@ws4.swamid

Verktygsbas

- SAML2test
- IdPproxy
- Native SAML2
  - ECP

SAML2test

- Verifiera att en SP/IdP/AA instans följer en speciell SAML2 profil

Test av

https://idp.umu.se/saml2/idp/metadata.php

1. Warning: "Metadata should contain contact person information"
2. Critical: "The IdP returns wrong NameID format"

IdPproxy

- Gateway mellan SAML2 och Social media
- Stöder nu
  - Google, Facebook, Twitter
- Snart
  - LiveID, LinkedIN, Paypal, ...

idp-test.social2saml.org

- Varje SP operatör registrerar sin applikation
- Paketerar erhållet client_id/client_secret par per service i en krypterad json struktur.

```
{
   "Google": {
      "key": "341592653589793",
      "secret": "fefafefafefafefafefafefafefafefa"},
}
```

- Skickar till mig

Typiskt resultat
Google

givenName: 'Johan',
displayName: 'Johan Lundberg',
uid: '113388788534379655753',
surname: 'Lundberg',
email: lundberg.johan@gmail.com
eduPersonTargetedID: 'https://idp-test.social2saml.org:8090/idp!http://crowdtest.nordu.net/shibboleth!590b52f29f1b75deea14d9e2fd36f412',
eduPersonPrincipalName: lundberg.johan@google.social2saml.org

Facebook

givenName: 'Johan',

displayName: 'Johan Lundberg',

uid: 'http://www.facebook.com/johan.lundberg.908'

surname: 'Lundberg',

e*mail*: 'lundberg@nordu.net',

eduPersonTargetedID: 'https://idp-test.social2saml.org:8090/idp!http://crowdtest.nordu.net/shibboleth!3c8282137c5de1ddf10bee6f32a8b4f1',

eduPersonPrincipalName: 'johan.lundberg.908@facebook.social2saml.org,

Twitter

displayName: 'Lundberg_J',

uid: '294600041',

eduPersonTargetedID: 'https://idp-test.social2saml.org:8090/idp!http://crowdtest.nordu.net/shibboleth!9121ba687870ca09443f64df5fa5c3ad',

eduPersonPrincipalName: 'Lundberg_J@twitter.social2saml.org'

‘Native’ SAML2

```
from saml2.client import Saml2Client


client = Saml2Client(config_file=”sp_config”)
outstanding = {}
id, ht_resp = client.do_authenticate(
                                ”https://idp.umu.se/saml2/idp/metadata.php”,
                                relay_state="foobar01")
outstanding.update({id:path})
....
resp = client.authn_request_response(post, outstanding)
```

ECP

Enhanced Client or Proxy Profile

- För applikationer/kommandoradsskript
- Freeradius backend - Moonshot