SAML2 testverktyg

Bakgrund

- För att en federation skall fungera bra krävs att alla ingående enheter följer:
  - SAML2 standarden
  - SAML2 profilen
  - Eventuella federationsöverenskommelser

Inblandade organisationer

- GEANT3/3+ (finansiering)
- Kantara
- Österrikiska regeringen

SAML2 profil

- saml2int
  - Metadata provided by both Identity Providers and Service Provider SHOULD contain contact information for support and for a technical contact.
  - Assuming a successful response, the `<saml2p:Response>` message issued by an Identity Provider MUST contain exactly one assertion

kmh.se {'organization_name': ['KMH'], 'contact_type': ['technical']}
user.uu.se {'organization_name': ['U'], 'display_name': ['Uppsala universitet'], 'contact_type': ['technical']}
oru.se {'organization_name': ['OR'], 'display_name': ['Örebro universitet'], 'contact_type': ['technical', 'technical']}
umu.se {'organization_name': ['Um', 'Um'], 'contact_type': ['technical']}
chalmers.se {'organization_name': ['CHALMERS'], 'contact_type': ['technical', 'technical', 'technical']}
hb.se {'organization_name': ['HB'], 'display_name': ['Högskolan i Borås'], 'contact_type': ['technical']}
mah.se {'organization_name': ['MAH'], 'contact_type': ['technical']}
hh.se {'organization_name': ['HH'], 'contact_type': ['technical']}
rkh.se {'organization_name': ['The Red Cross University College'], 'contact_type': ['technical']}
hig.se {'organization_name': ['HIGALUMNI'], 'display_name': ['Högskolan i Gävle (Alumni)'], 'contact_type': ['technical']}
ltu.se {'organization_name': ['LT'], 'contact_type': ['technical']}
bth.se {'organization_name': ['BTH'], 'contact_type': ['technical']}
liu.se {'organization_name': ['Li'], 'display_name': ['Linköpings universitet'], 'contact_type': ['administrative', 'support', 'technical']}
ki.se {'organization_name': ['KI'], 'contact_type': ['technical']}
du.se {'organization_name': ['D'], 'display_name': ['Högskolan Dalarna'], 'contact_type': ['technical']}
hkr.se {'organization_name': ['HKR'], 'contact_type': ['technical']}
vhs.se {'organization_name': ['VHS'], 'contact_type': ['technical']}
mdh.se {'organization_name': ['MDH'], 'display_name': ['Mälardalens högskola'], 'contact_type': ['technical']}
miun.se {'organization_name': ['MIUN'], 'contact_type': ['technical']}
irf.se {'organization_name': ['IRF'], 'contact_type': ['technical']}
ecsidp.antagning.se {'organization_name': ['UHR'], 'contact_type': ['technical']}
su.se {'organization_name': ['S'], 'display_name': ['Stockholms universitet'], 'contact_type': ['technical']}
gu.se {'organization_name': ['G'], 'display_name': ['Göteborgs universitet'], 'contact_type': ['technical']}
hj.se {'organization_name': ['HJ'], 'display_name': ['Högskolan i Jönköping'], 'contact_type': ['technical']}
kb.se {'organization_name': ['KB'], 'contact_type': ['technical']}
kth.se {'organization_name': ['KTH'], 'contact_type': ['technical']}
vr.se {'organization_name': ['VR'], 'contact_type': ['technical']}
kau.se {'organization_name': ['KA'], 'display_name': ['Karlstads universitet'], 'contact_type': ['technical', 'technical']}
slu.se {'organization_name': ['Swedish University of Agricultural Science'], 'contact_type': ['technical', 'administrative', 'support']}
lnu.se {'organization_name': ['LN'], 'display_name': ['Linnéuniversitetet'], 'contact_type': ['technical']}
konstfack.se {'organization_name': ['Konstfack'], 'contact_type': ['technical']}

Varför?

- [ ] idag
- [ ] Inkludera enheten (SP/IdP/AA) och se vad som händer

- [ ] I morgon
  - [ ] Innan enheter släpps in i federation testas de m.h.a testverktyget.
  - [ ] OK krävs på alla testerna för att få delta.

Vad man kan råka ut för

- [ ] No metadata
- [ ] Only endpoint + certificate
- [ ] Kräver ‘saml2p’ not ‘samlp’

They send:

```
<samlp:Response Destination="http://spexample.com/saml2/acs/" ID="1100164796"
                IssueInstant="2013-05-15T12:35:40.724Z" Version="2.0">
   <ds:Signature>
       <ds:SignedInfo>
```

What they should have sent:

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                Destination="http://spexample.com/saml2/acs/" ID="1100164796"
                IssueInstant="2013-05-15T12:35:40.724Z" Version="2.0">
   <ds:Signature>
       <ds:SignedInfo>
```

Vad?

- [ ] Att enheten följer reglerna
- [ ] Felhantering
- [ ] Kända attackvektorer

Design

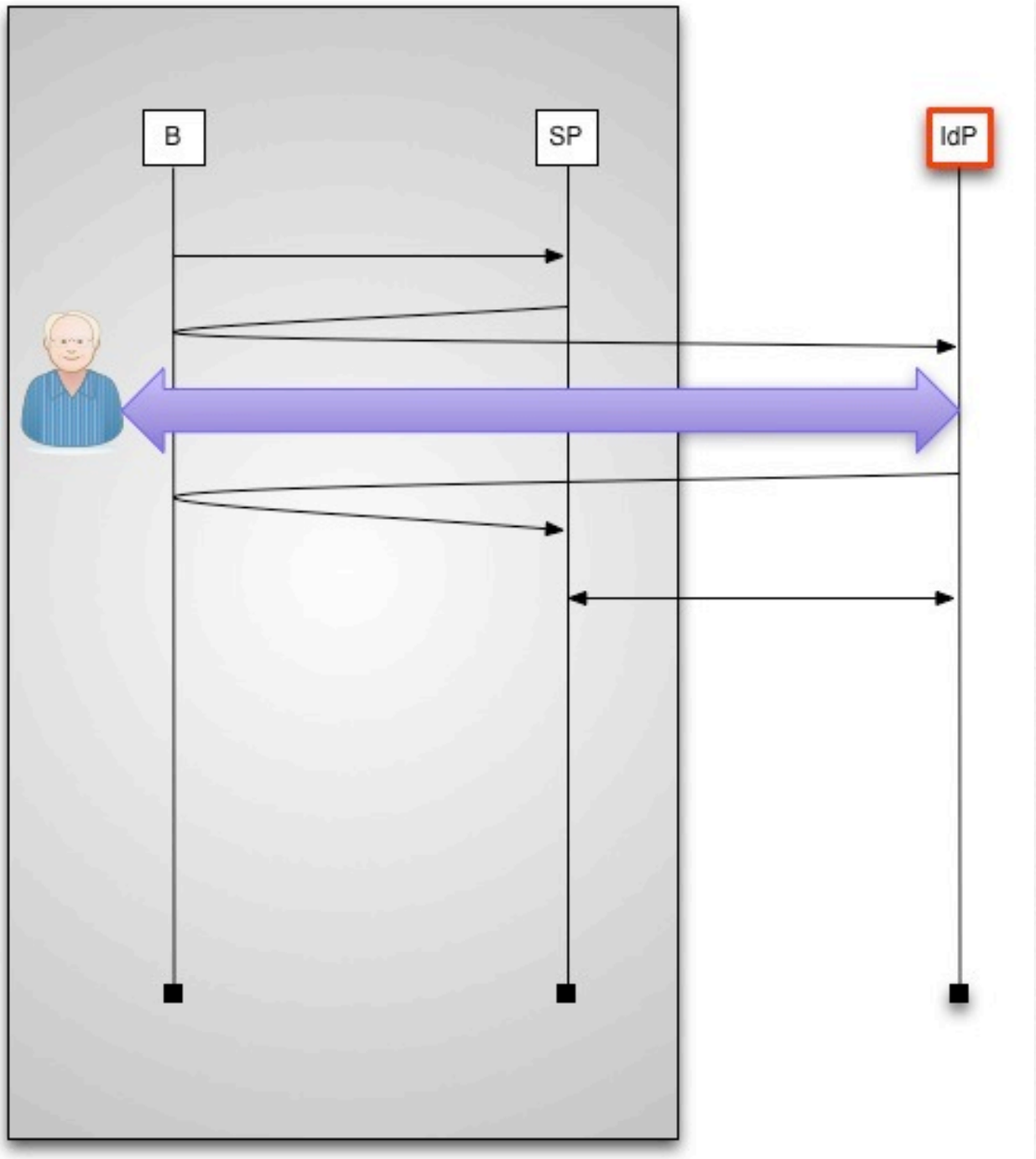
- Front-end som hanterar all interaktion med användare
  - http://openidtest.uninett.no
- Back-end hanterar all kommunikation med den testade enheten
  - implementerad som ett skript

Hur?

Test struktur

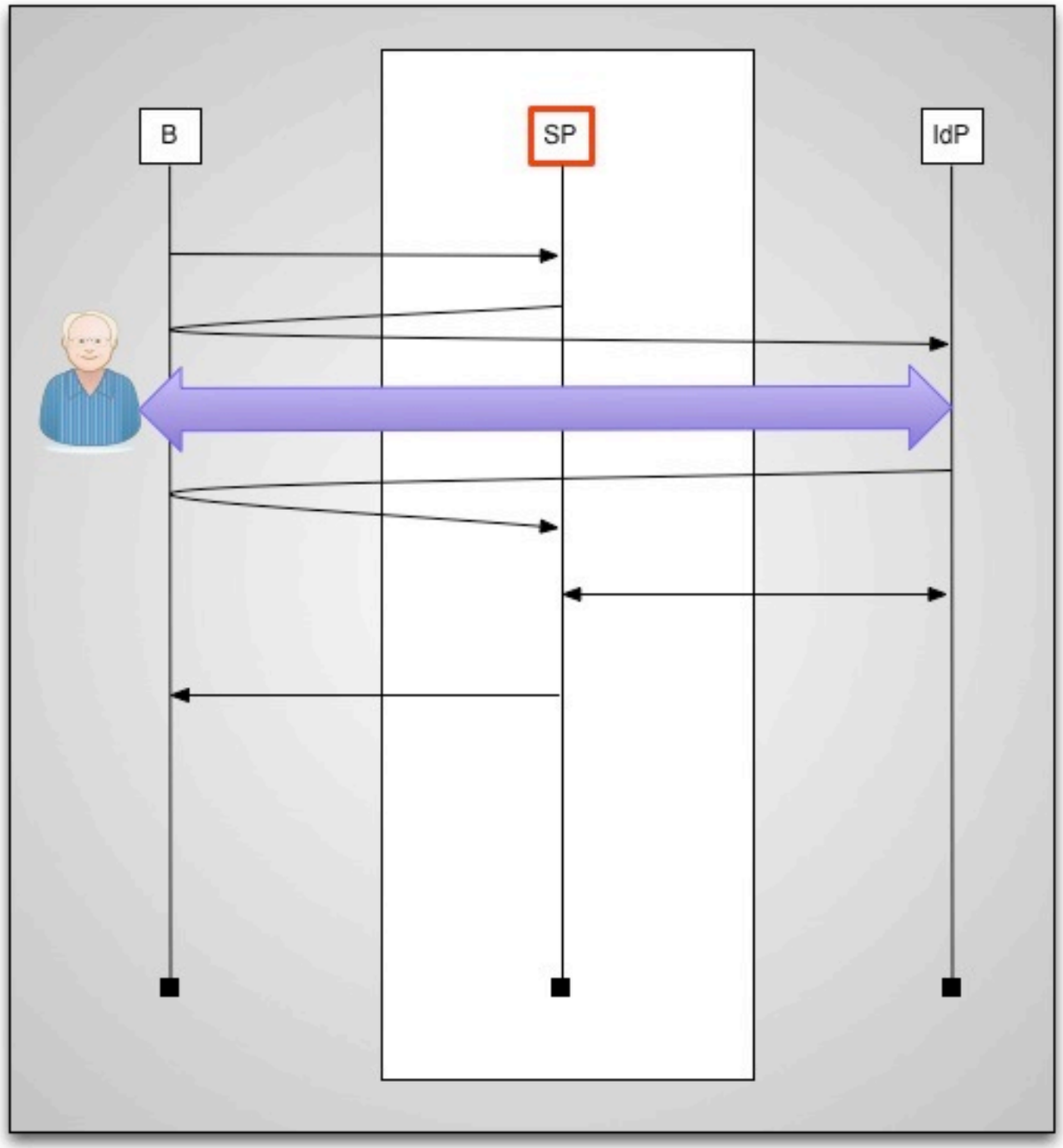
- En test är en konversation med tillhörande tester
- En konversation är en sekvens av request-response par
- varje meddelande kan föregås eller följas av ett set tester.

- Test av en IdP
- Verktyget agerar användare, webläsare och SP

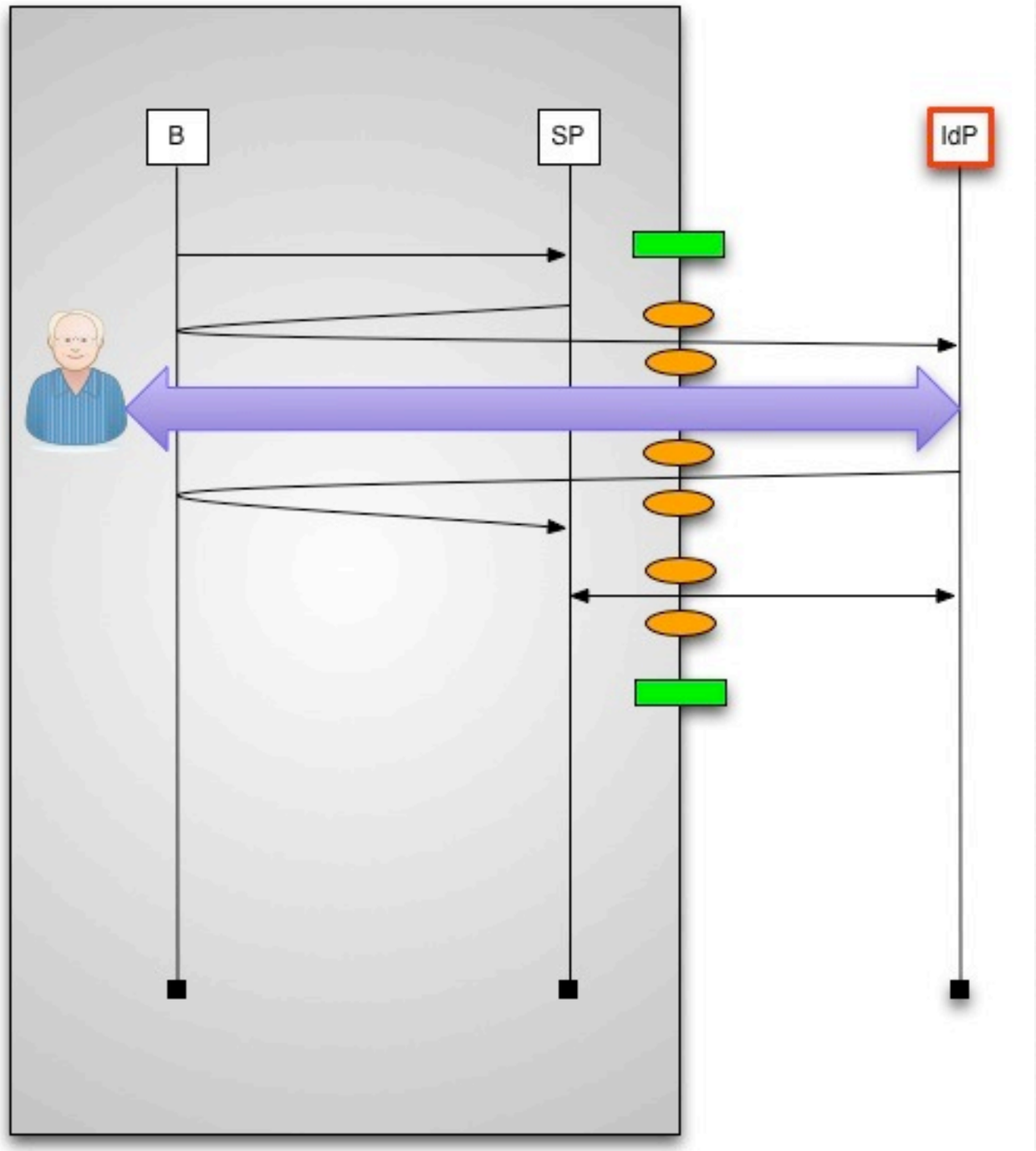


- Test av en SP

- Verktyget agerar användare, webläsare och IdP



- Tester under en konversation



Exempel

Koden

- https://github.com/rohe/saml2test

Konfigurations exempel

```
#!/usr/bin/env python
__author__ = 'rolandh'

import json

BASE = "https://testshib.portalverbund.at"

metadata = open("./testshib-md.xml").read()
```

```
info = {
    "entity_id": "%s/idp/shibboleth" % BASE,
    "interaction": [
        {
            "matches": {
                "url": "%s/idp/Authn/UserPassword" % BASE,
                "title": 'Shibboleth Identity Provider'
            },
            "page-type": "login",
            "control": {
                "type": "form",
                "set": {"login": "test@bmspot.gv.at", "password": "test"}
            }
        },
        {
            "matches": {
                "url": "%s/sso/redirect" % BASE,
                "title": "SAML 2.0 POST"
            },
            "control": {
                "type": "response",
                "pick": {"form": {"action":"%s/acs" % BASE}}
            }
        },
    ],
    "metadata": metadata
}

print json.dumps(info)
```

$ saml2c.py -J localhost.json "authn"

{"status": 1, "id": "check-saml2int-metadata", "name": "Checks that the Metadata follows the Saml2Int profile"},

{"status": 1, "id": "check", "name": "Verifies that the IdP supports the needed functionality"},

{"status": 1, "id": "check-saml2int-attributes", "name": "Any <saml2:Attribute> elements exchanged via any SAML 2.0 messages, assertions, or metadata MUST contain a NameFormat of urn:oasis:names:tc:SAML:2.0:attrname-format:uri."},

{"status": 1, "id": "verify-attribute-name-format", "name": "Verify that the correct attribute name format is used."},

{"status": 1, "id": "check", "name": "verify that the correct part was signed."},

{"status": 1, "id": "check", "name": "verify that the used signature algorithm was one from an approved set."}

0.011537 SAML Request: <?xml version='1.0' encoding='UTF-8'?>

<ns0:AuthnRequest xmlns:ns0="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:ns1="urn:oasis:names:tc:SAML:2.0:assertion" AssertionConsumerServiceURL="http://localhost:8087/acs/post" Destination="http://localhost:8088/sso/redirect" ID="id-04bef4f068e3f80c135c66cf2d8726d3" IssueInstant="2013-04-16T07:42:31Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" ProviderName="SAML2 test tool" Version="2.0"><ns1:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://localhost:8087/sp.xml</ns1:Issuer><ns0:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" /></ns0:AuthnRequest>

0.026832 <-- REDIRECT TO: http://localhost:8088/login?came_from=%2Fsso%2Fredirect&key=0e0cff37176640a99c3449ed2251b463ded08aaf

0.029497 <-- CONTENT:

<html>

... snip...

</html>

0.032119 >> login <<

0.032139 <-- FUNCTION: select_form

0.032155 <-- ARGS: {'set': {'login': 'roland', 'password': 'dianakra'}, 'location': 'http://localhost:8088/login?came_from=%2Fsso%2Fredirect&key=0e0cff37176640a99c3449ed2251b463ded08aaf', 'type': 'form', 'features': None}

0.038400 <-- REDIRECT TO: http://localhost:8088/sso/redirect?id=P42MidQTDuXPL6ph2QMZxRiL&key=0e0cff37176640a99c3449ed2251b463ded08aaf

0.045512 <-- CONTENT: <head><title>SAML 2.0 POST</title></head><body><form method="post" action="http://localhost:8087/acs/post">

<input type="hidden" name="SAMLResponse" value="PD94bWwg....."

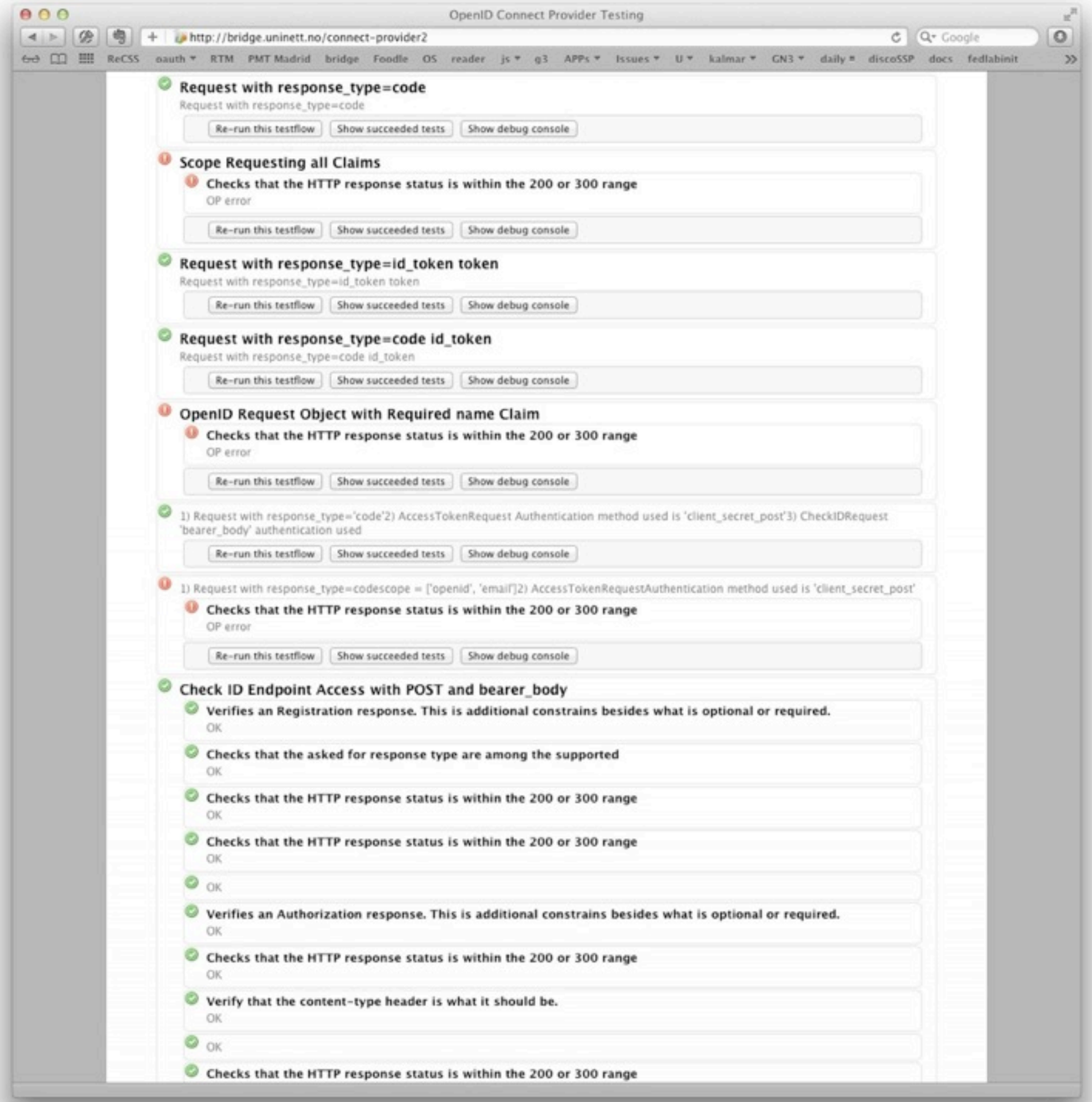
0.046434 >> other <<

0.046451 <-- FUNCTION: select_form

0.046466 <-- ARGS: {'index': 0, 'set': {}, 'location': 'http://localhost:8088/sso/redirect?id=P42MidQTDuXPL6ph2QMZxRiL&key=0e0cff37176640a99c3449ed2251b463ded08aaf', 'type': 'form', 'features': None}

0.053179 SAML Response: <?xml version='1.0' encoding='UTF-8'?>

<ns0:Response


OpenID Connect Provider Testing
http://bridge.uninett.no/connect-provider2
Request with response_type=code
Request with response_type=code
Re-run this testflow
Show succeeded tests
Show debug console
Scope Requesting all Claims
Checks that the HTTP response status is within the 200 or 300 range
OP error
Request with response_type=id_token token
Request with response_type=id_token token
Request with response_type=code id_token
Request with response_type=code id_token
OpenID Request Object with Required name Claim
Checks that the HTTP response status is within the 200 or 300 range
OP error
1) Request with response_type='code'2) AccessTokenRequest Authentication method used is 'client_secret_post'3) CheckIDRequest 'bearer_body' authentication used
1) Request with response_type=codescope = ['openid', 'email']2) AccessTokenRequestAuthentication method used is 'client_secret_post'
Checks that the HTTP response status is within the 200 or 300 range
OP error
Check ID Endpoint Access with POST and bearer_body
Verifies an Registration response. This is additional constrains besides what is optional or required.
OK
Checks that the asked for response type are among the supported
OK
Checks that the HTTP response status is within the 200 or 300 range
OK
Checks that the HTTP response status is within the 200 or 300 range
OK
OK
Verifies an Authorization response. This is additional constrains besides what is optional or required.
OK
Checks that the HTTP response status is within the 200 or 300 range
OK
Verify that the content-type header is what it should be.
OK
OK
Checks that the HTTP response status is within the 200 or 300 range