How to set up a federated SAML Service Provider

Arsen Hayrapetyan, SCC, KIT

Glossary

- **SAML** is a standard which defines a framework for exchanging authentication and authorisation information between parties, in particular Service Provider (SP) and Identity Provider (IdP)
- **SAML IdP**: An entity authenticating the users and providing assertions containing information about users' identities and additional attributes to the SP
- **SAML SP**: An entity providing services to users, that makes access control decisions based on the assertions from the IdP
- **SAML-based Federation**: An entity that serves common interests of the IdP home organisations and SPs and establishes trust relationship between members of the federation.

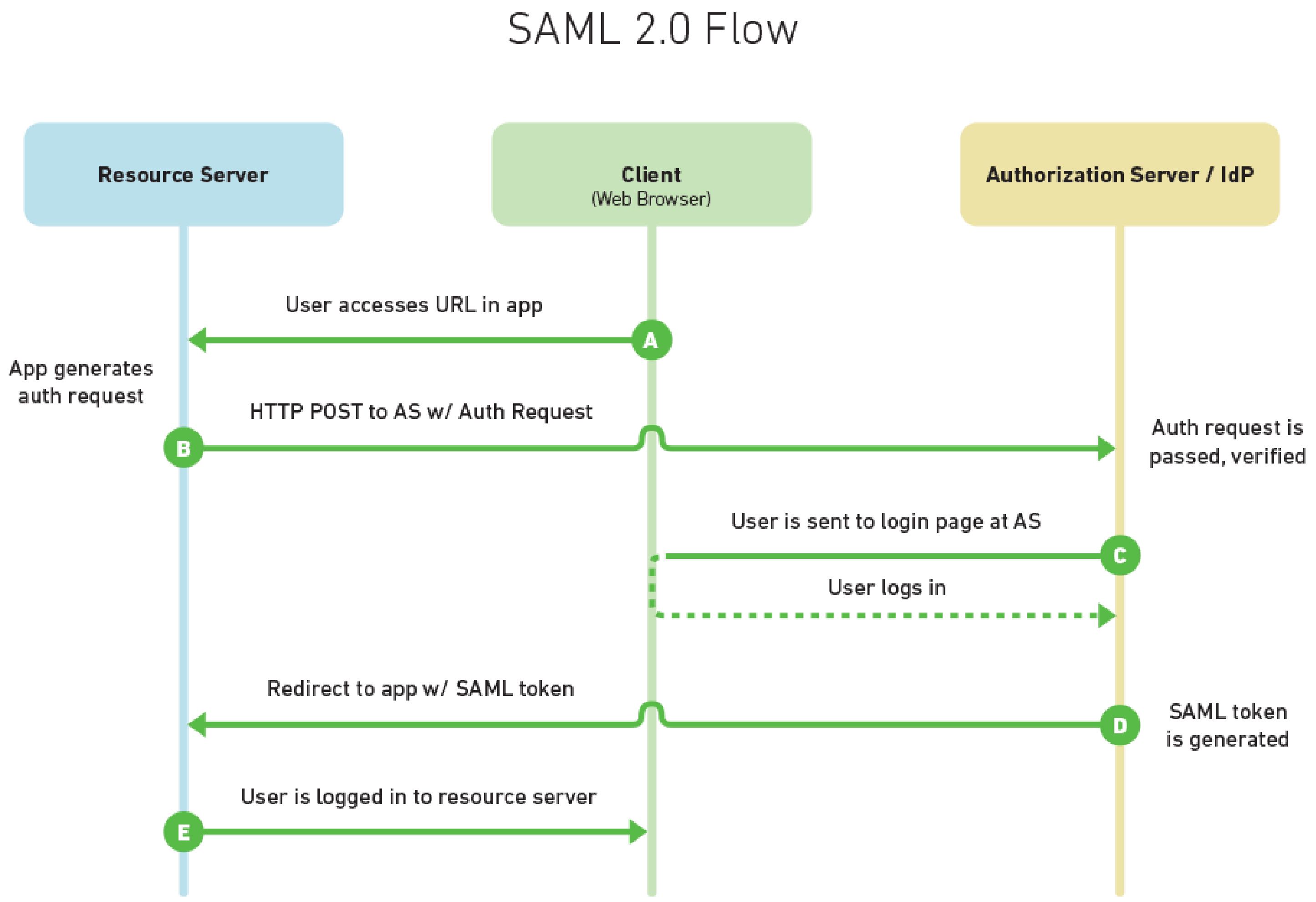
SAML-based Identity Federations: DFN-AAI

- The German Research Network (Deutsches Forschungsnetz, DFN) manages two identity federations:
  - DFN-AAI (production)
  - DFN-AAI-Test (test)

- DFN-AAI services
  - Drawing up contracts
  - Establishment and maintenance of guidelines (policies)
  - Operating a central Discovery Service
  - Metadata management
  - Support in case of technical problems
  - Training for its members

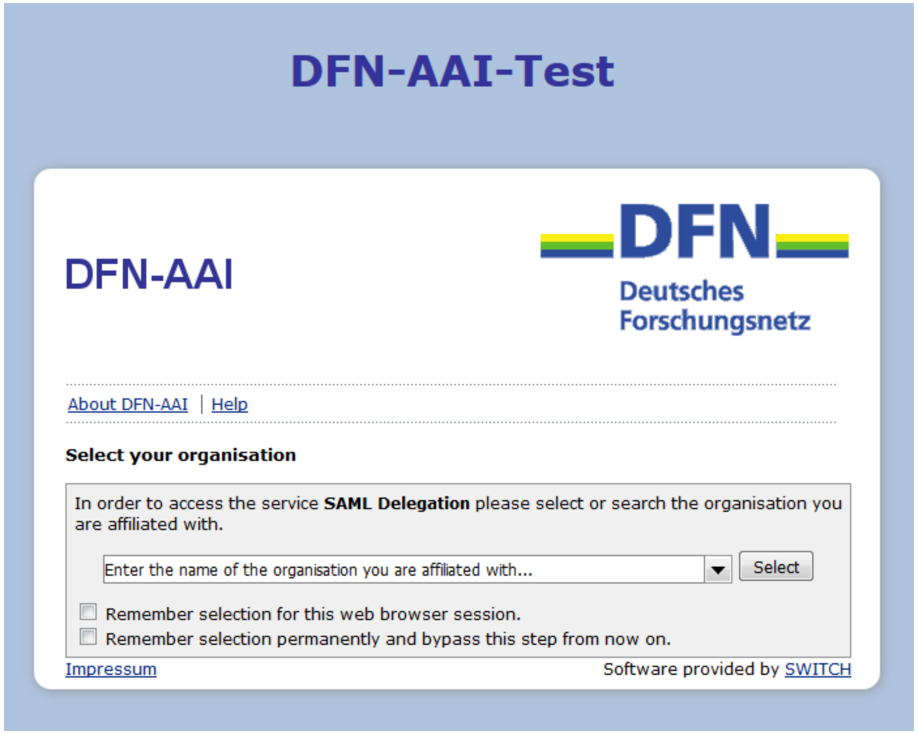
https://www.aai.dfn.de/en/der-dienst/federation/

Typical access flow in a SAML-based system


SAML 2.0 Flow
Resource Server
Client
(Web Browser)
Authorization Server / IdP
User accesses URL in app
A
App generates auth request
HTTP POST to AS w/ Auth Request
B
Auth request is passed, verified
User is sent to login page at AS
C
User logs in
Redirect to app w/ SAML token
D
SAML token is generated
User is logged in to resource server
E

WAYF service

- Enables the users to select their Home Organisation for the authentication when redirected to the IdP by the SPP
  - Provided by the Federation
    - DFN AAI
    - DFN Test-AAI



DFN-AAI-Test

Select your organisation

In order to access the service **SAML Delegation** please select or search the organisation you are affiliated with.

Enter the name of the organisation you are affiliated with... Select

□ Remember selection for this web browser session.

□ Remember selection permanently and bypass this step from now on.

Impressum

Software provided by SWITCH

Road map for a DFN-AAI-federated SAML SP

- Defining the list of user attributes that will be to make the authorisation decision
- Installing SAML SP software and auxiliary software
- Requesting and installing a host certificate for the SP
- Configuring the SAML SP software
  - SP “entity endpoint”
  - WAYF service location
  - ECP (for a non web-based service). Your IdP(s) have to support ECP to make it work!
- Registering your SP metadata with the test Federation and testing it
- Signing Federation’s SP agreement
- Registering your metadata with the production Federation and enabling the SP

Attribute release

- KIT IdP, KIT Test IdP
  - eduPersonPrincipalName, Entitlement, Affiliation, PersistentID
- Where can I find out which attributes does IdP release?
  - In general there is no general answer
  - An SP can request a set of attributes
  - Every IdP may decide to release **ANY** set of attributes
  - Any assumption by the SP is likely to fail
    - To fail one day
    - To fail without prior notice
    - To fail depending from which IdP the user comes
    - There are about 7000 IdPs in the world today

=> Do not request many attributes!

=> Do not make any assumptions

=> Federation policies will differ from country to country!

SAML SP installation (Ubuntu)

- Auxiliary software

```
apt-get update apt-get install ntp sudo curl apache
```

- Shibboleth SP

```
$> gpg --with-fingerprint SWITCHaai-swdistrib.asc
$> apt-key add SWITCHaai-swdistrib.asc
$> echo 'deb http://pkg.switch.ch/switchaai/debian wheezy main' >> \
/etc/apt/sources.list.d/SWITCHaai-swdistrib.list
$>apt-get update
$>apt-get install shibboleth
```

- Certificate
  - /etc/ssl/host[cert|key].pem
- Documentation:
  - SWITCH AAI: https://www.switch.ch/aai/docs/shibboleth/SWITCH/latest/sp/deployment/

SAML SP configuration

- shibboleth2.xml file

```
<ApplicationDefaults entityID=https://saml-delegation.data.kit.edu/shibboleth
                    REMOTE_USER="eppn persistent-id targeted-id" >
```

```
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
            checkAddress="false" handlerSSL="true" cookieProps="https"
            exportLocation="/GetAssertion"
            exportACL="141.52.160.10">
```

```
<SSO type="SAML2" Location="/ECP" ECP="true"
                discoveryProtocol="SAMLDS" discoveryURL="https://wayf.aai.dfn.de/DFN-AAI-Test/wayf">
              SAML2 SAML1
            </SSO>
```

SAML SP configuration

- /etc/apache2/sites-enabled/000-default-ssl.conf

```
<Location /secure>
      AuthType shibboleth
      ShibRequestSetting requireSession 1
      require valid-user
</Location>
```

- Putting the app in the /secure dir
- Documentation:
  - SWITCH AAI: https://www.switch.ch/aai/docs/shibboleth/SWITCH/latest/sp/deployment/

Adding your SP metadata to the Federation

- Your SP metadata is normally auto-generated
- Adding SP metadata to the Federation metadata according to the Federation rules
  - DFN offers
    - admin account to SP administrators to manage their data
    - Sending the data in to be added by DFN operators manually

Example: https://saml-delegation.data.kit.edu

- Go to the page