PAUL SCHERRER INSTITUT

PSI

Björn Erik Abt :: IT Security Officer :: Paul Scherrer Institut

SSO – The SAML2 Flow

04.02.2021

PAUL SCHERRER INSTITUT

Agenda

- **History**
- **Federations**
- **Components**
  - Identity Provider
  - Service Provider
  - Discovery Service
- **Terminology**
- **Communication Flow**

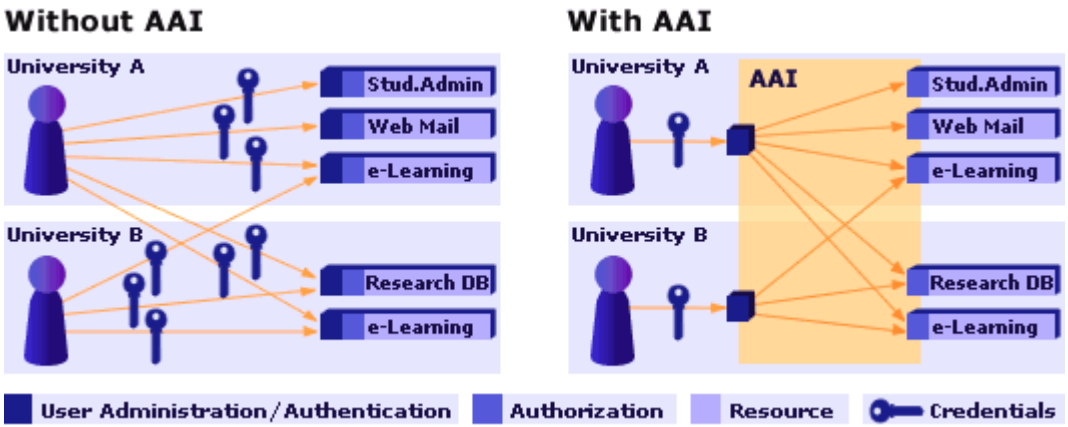
History of SAML

- **November 2002**: **SAML v1.0** becomes an OASIS standard
- **September 2003**: **SAML v1.1** released
  - SAML had a significant success, gaining momentum in financial services, higher education, government, and other industry segments.
- **March 2005**: **SAML v2.0** released
  - SAML V2.0 unifies the building blocks of federated identity in SAML V1.1 with input from higher education's Shibboleth initiative and the Liberty Alliance's Identity Federation Framework.
  - SAML V2.0 is a critical step towards full convergence for federated identity standards.

Source: OASIS (Organization for the Advancement of Structured Information Standards)

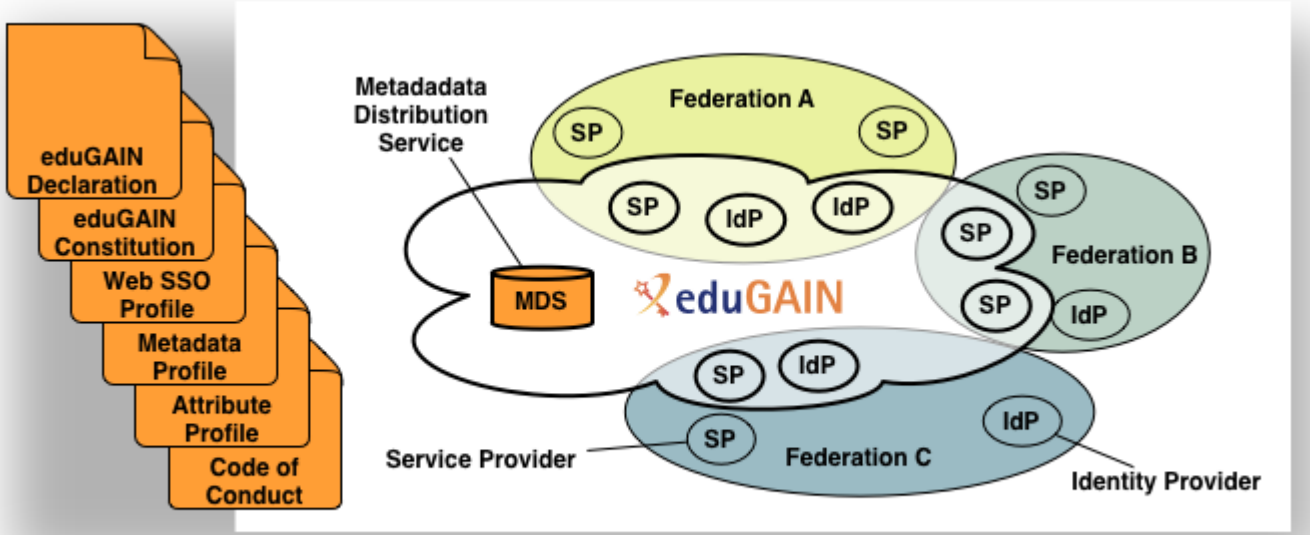
Federations

- **NREN (National Research and Education Network)**
  - They host national services which provide universities and research institutes with a federated AAI
  - Make it much easier to share resources between entities



Federations

- **eduGAIN**
  - A international federation of federations operated by GÉANT



Federations

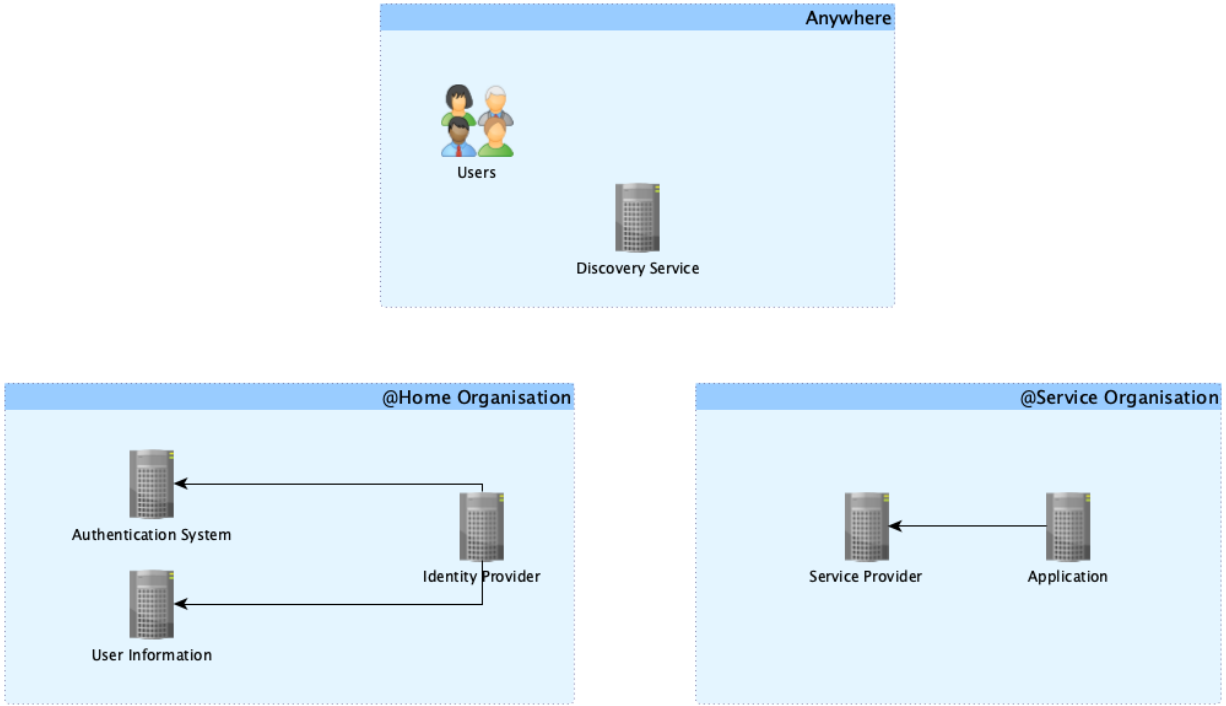
- **Countries with a NREN based federation**

Source: refeds.org

Components

So, what are the components to build a SAML federation?

Components


Anywhere
Users
Discovery Service
@Home Organisation
Authentication System
Identity Provider
User Information
@Service Organisation
Service Provider
Application

Components: Identity Provider (IdP)

- Authenticates users and provides information about users (attributes)
- Connects to existing authentication and user data systems
- Provides information about how a user has been authenticated
- Provides user identity information from the data source

Components: Service Provider (SP)

- Component handling the SAML protocol and protecting the web application, typically running on the same serve as the web application itself.
- Initiates the request for authentication and attributes
- Processes incoming authentication and attribute information (SAML assertion from IdP)
- Optionally evaluates content access control rules
- Passes user information (attributes) to web application

Components: Discovery Service (DS)

- Lets the user choose the home organization the user belongs to
- Tells the Service Provider which Identity Provider to use for authentication and attribute retrieval
- Can be integrated into the web resource or used as a separate central service
- Also known as "WAYF" (Where Are You From) service

Terminology

- **SAML - Security Assertion Markup Language**
  - The OASIS standard describing the XML messages exchanged between IdP and SP (two versions: 1.1, 2.0)

- **Profile**
  - Standard describing how to use SAML messages to accomplish a specific task (e.g. SSO, attribute query)

- **Binding**
  - Standard that describes how to take a profile message and send it over a specific transport (e.g. HTTP)

Terminology

- **entityID**
  - Unique identifier for an IdP or SP
  - Examples:
    - IdP: https://aai-login.example.org/idp/shibboleth
    - SP: https://moodle.example.org/shibboleth
- **NameID**
  - An identifier by which an IdP knows a user
  - Examples:
    - 234567@example.org
    - https://aai-login.example.org/idp/shibboleth!https://moodle.example.org/shibboleth!dlFC71fyChS8kGdgYcacD3uoDOQ=

Terminology

- **Attribute**
  - A named piece of information about a user
  - Examples:
    - givenName: John
    - surname: Doe
    - homeOrganization: example.org

Terminology

- Assertion
  - The unit of information in SAML
  - Example:

```
<saml:Assertion ...>
        <saml:Issuer ...>https://aai6login.example.org/idp/shibboleth</saml:Issuer>
        <saml:Subject ...>
                <saml:NameID ...>_e7b68a04488f715cda642fbdd90099f</saml:NameID>
        </saml:Subject>
        <saml:AuthnStatement ....>.....</saml:AuthnStatement>
        <saml:AttributeStatement ...>
                [...] (Attributes)
        </saml:AttributeStatement>
</saml:Assertion>
```

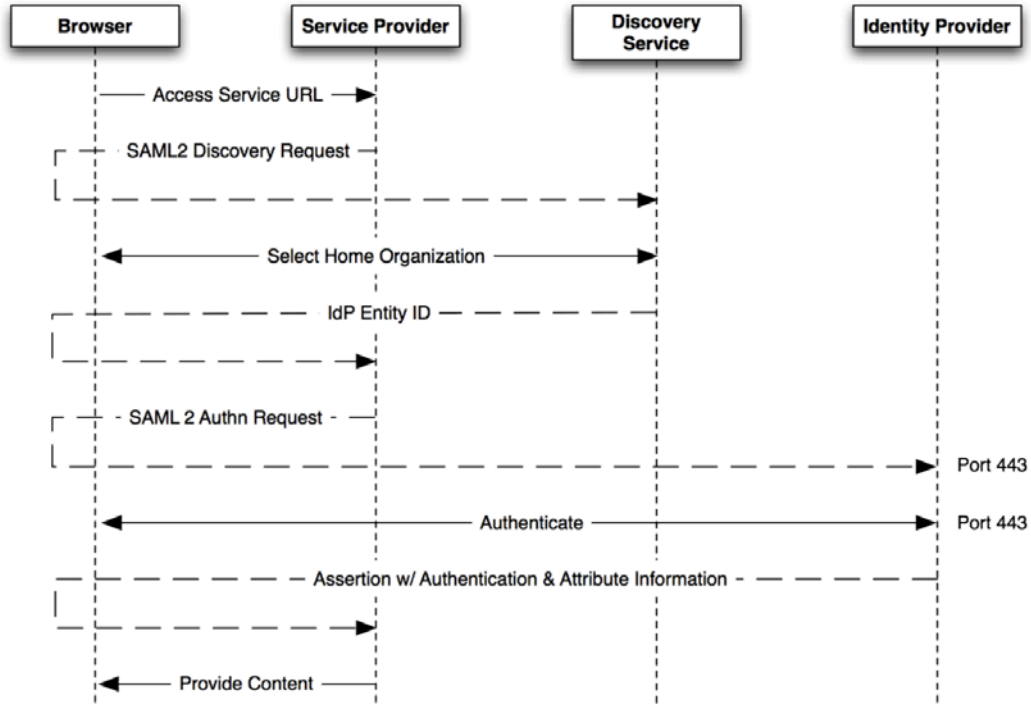
Terminology

- **Service / Resource**
  - Application that supports SAML (e. g. Useroffice, Keycloak etc.)

- **Service Provider**
  - SAML component running on the application's server providing SAML support for the application

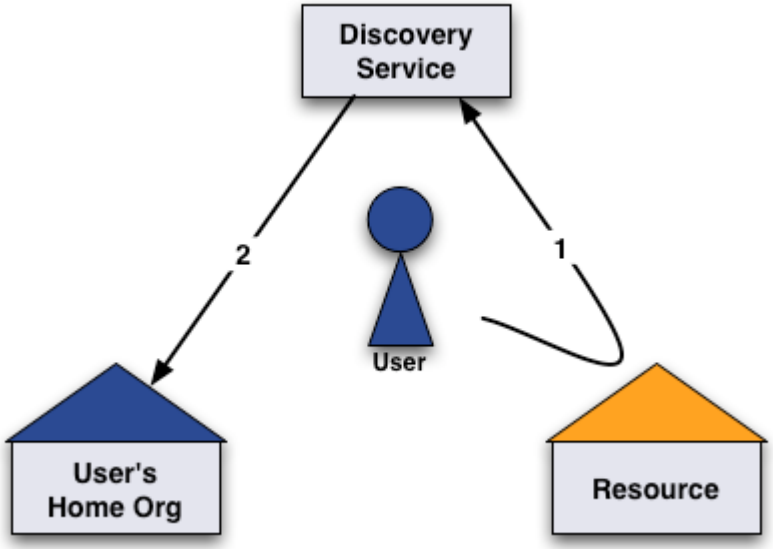
- **SAML Metadata**
  - A SAML metadata document describes a SAML deployment such as a SAML identity provider or a SAML service provider. Deployments share metadata to establish a baseline of trust and interoperability.

SAML2 SSO Webflow



Source: www.switch.ch

SAML2 SSO Webflow - Overview



Source: www.switch.ch

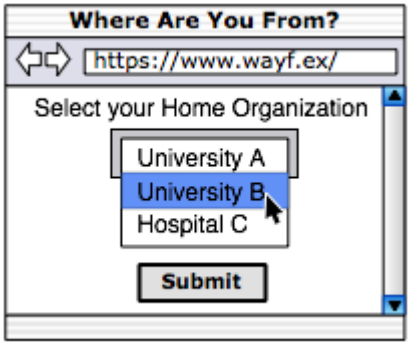
SAML2 SSO Webflow

- **User connects to resource and is redirected**

Source: www.switch.ch

SAML2 SSO Webflow

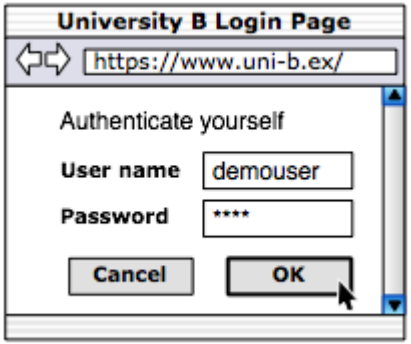
- **Home organisation selection**



Source: www.switch.ch

SAML2 SSO Webflow

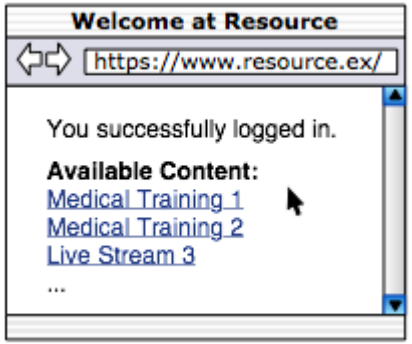
- **User authentication at home Identity Provider**



Source: www.switch.ch

SAML2 SSO Webflow

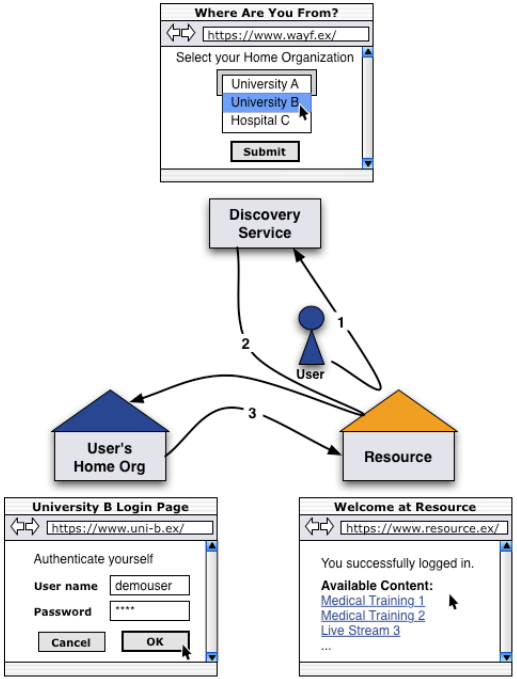
- **Access to resource granted and attributes transfered**



Source: www.switch.ch

SAML2 SSO Webflow

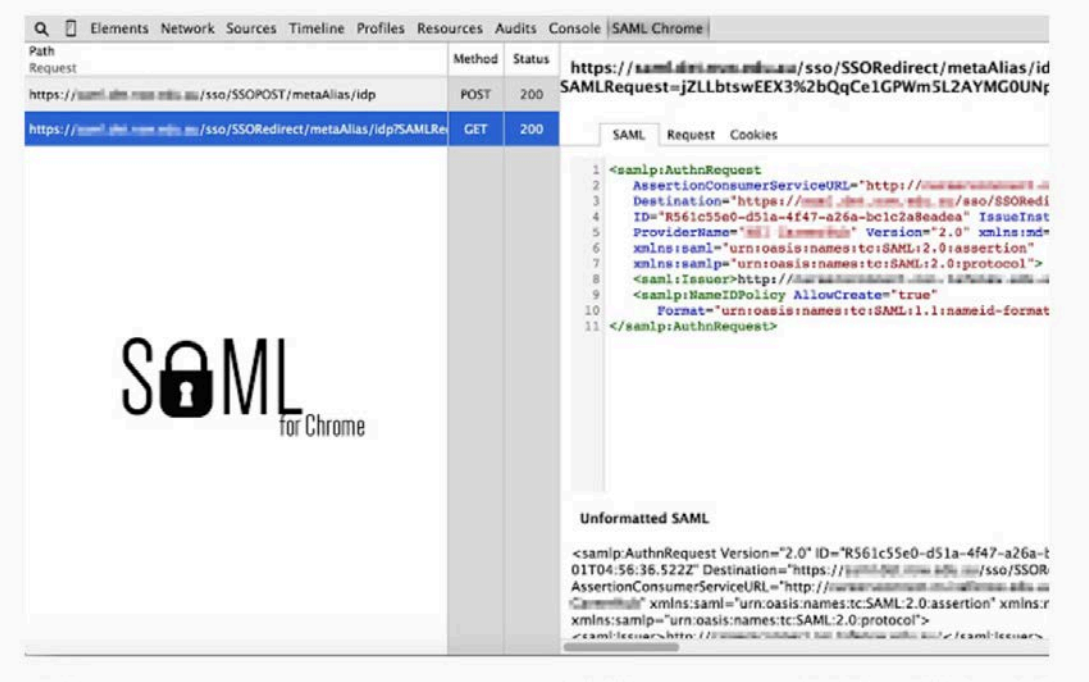
- **Summary: The login procedure**



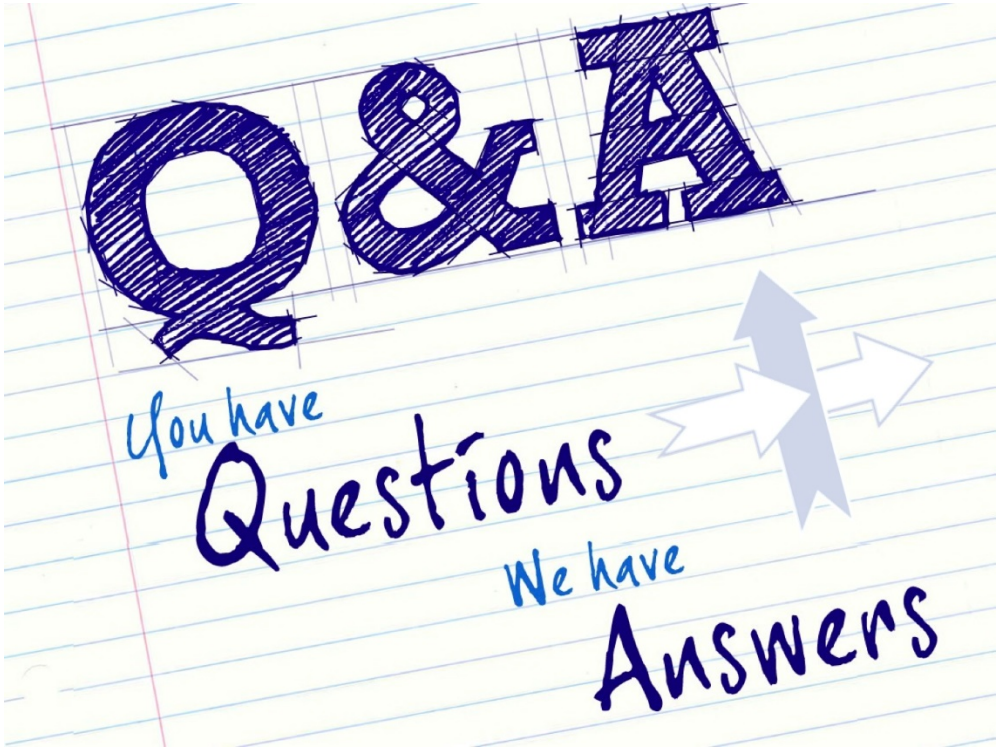
Source: www.switch.ch

Debug

- All trafic is end-to-end encrypted so it is very difficult to intercept!
- Debugging on the IdP:
  - Logfiles
- Debugging on the SP:
  - Logfiles
- Debugging in the Browser:



Questions & Answers



Thank you very much!