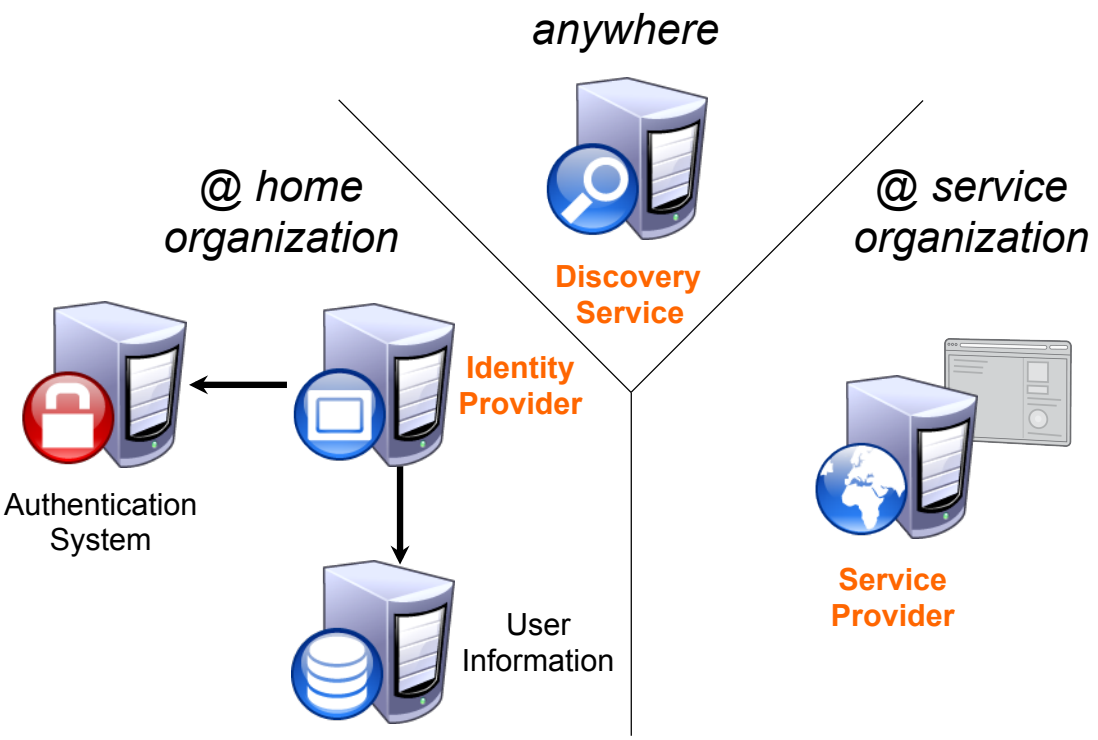
SAML Terminology & Flows

SWITCHaai Team
aai@switch.ch

Agenda

- Components
- Terminology
- Communication Flow

Components



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 (1)

- 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 (2)

- 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=`
  - `_e7b68a04488f715cda642fbdd90099f5`

Terminology (3)

- Attribute - A named piece of information about a user

  Examples:
  - givenName: `John`
  - surname: `Doe`
  - homeOrganization: `example.org`

- Assertion - The unit of information in SAML

  Example:

```
<saml:Assertion ...>
  <saml:Issuer ...>https://aai-login.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 (4)

- Service / Resource
  Application that supports SAML
  (e. g. Moodle, Ilias, etc.)

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

- "Shibbolized" application
  Application whose access is protected by SAML/Shibboleth

Communication Flow: SAML 2 SSO