PAUL SCHERRER INSTITUT

PSI

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

umbrellaID – Integration into your Application

04.02.2021

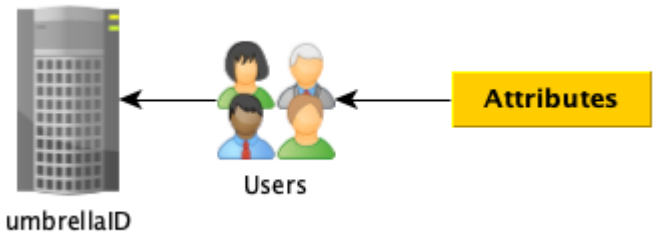
PAUL SCHERRER INSTITUT

Agenda

- **Architecture**
- **Flows**
  - Lookup umbrellaID: Session-Check
  - User check
  - User mapping

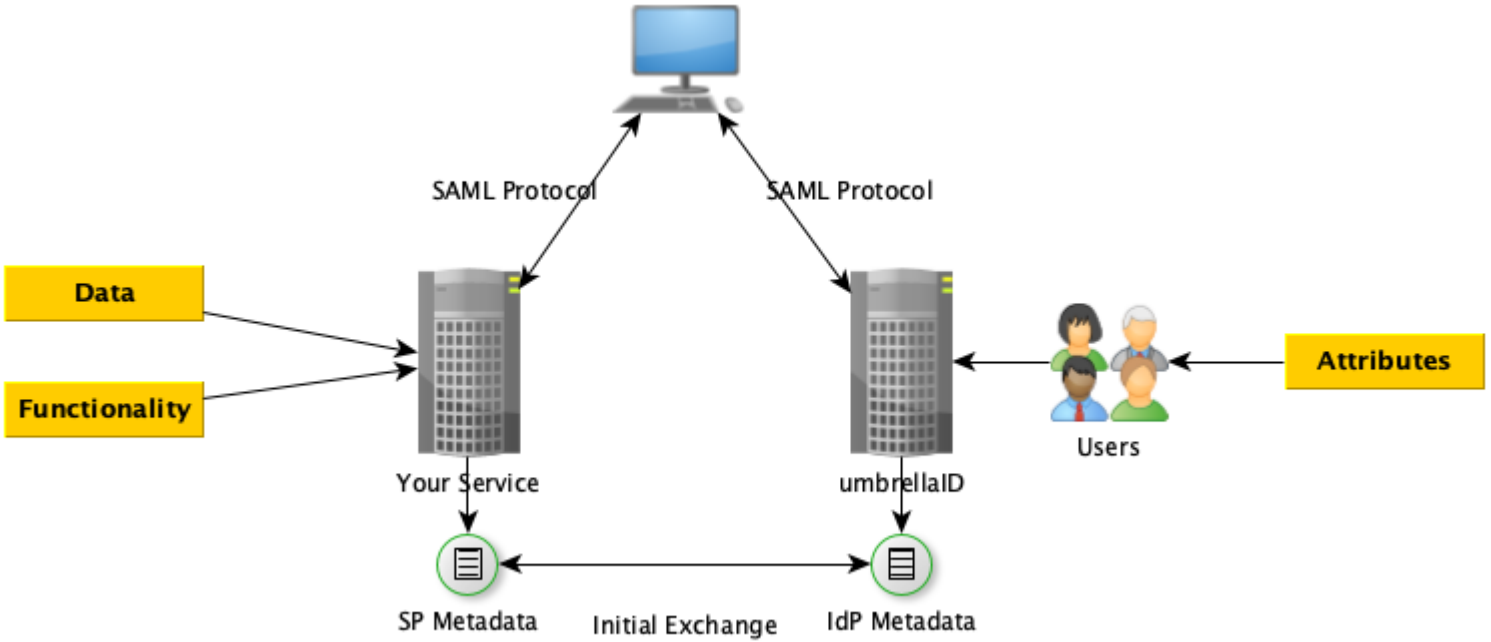
- **Attributes**
  - Accessing attributes
  - Attributes available

Architecture



Architecture

Architecture

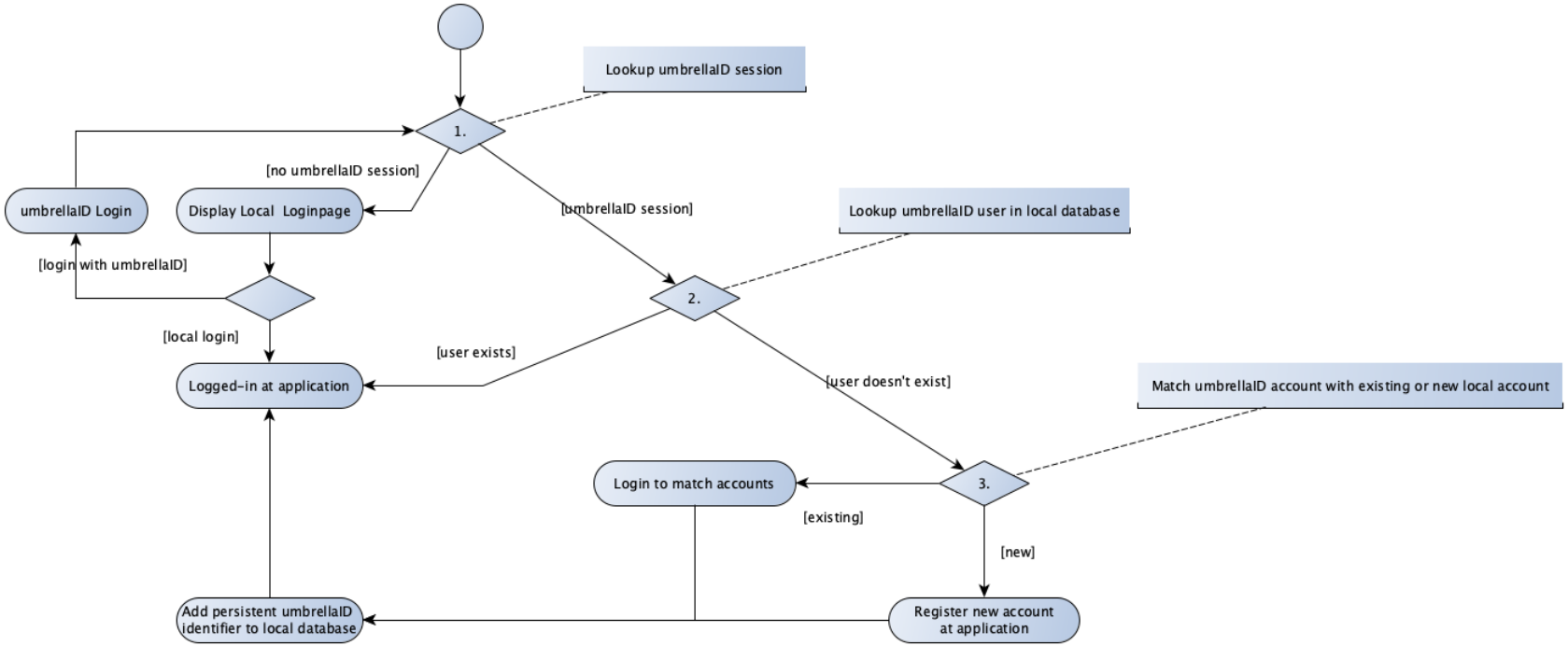


Flows

- It is presumed that following procedures are already installed at an application as this integration builds upon them:
  - Login Form
  - Create Account Form
- The Login Form is shown to incoming Umbrella-Users who have a Local-Account to let them match the two accounts.
- The Create Account Form is shown to incoming Umbrella-Users who don't have a Local-Account to let them create a new account according to the guidelines of the application.

PAUL SCHERRER INSTITUT

Flows



Flows

1. Umbrella-Session Check: Check if there is an existing Umbrella - Session active. If there is no valid Umbrella -Session, continue with the normal application code. Else forward the user to User Check.
2. User Check: Query the database for the incoming Umbrella-Hash. If there is a matching user, log him in. Else forward the user to User Matching.
3. User Matching: Let the user choose to match his Umbrella-Account with an existing WUO-Account or let him create a new account.

Flows: Umbrella-Session Check

- To find out if a user has a session, we need to read HTTP server headers for the attribute EAAHash:

Language	Construct
PHP	$_SERVER[“EAAHash”];
Java	httpServletRequest.getHeader(“EAAHash”);

- If this attribute is present, there is a session with umbrellaID

Flows: User Check

- The User Check consists basically of an extension to the SQL SELECT statement which besides querying for username and password also queries for the incoming EAAHash.

- Following code snippet (red and bold) can be used to enhance this generic user query:

```
SELECT
        USERNAME
FROM USERS
WHERE
        (USERNAME='user' AND PASSWORD='changeit')
OR
        (EAAHASH='f5bba3c6-6240-4ccf-8048-13dbb3405192')
```

Flows: User Matching

- User Matching is necessary if there is an incoming Umbrella-Session but no local user registered with it. It's important to use the existing “Login” and “Create User” procedures already installed at the application, so that no new procedures must be installed and approved.
- There is a chance that the user already has an existing account at the application and that the user wants to bind those accounts together – then a application login is performed and if successful, the found user tuple is enhanced in the USERS table with the incoming EAAHash.

Flows: User Matching

- To map an incoming umbrellaID with an existing local user following SQL statement can help as an example:

```
UPDATE
        USERS
SET
        EAAHASH='f5bba3c6-6240-4ccf-8048-13dbb3405192'
WHERE
        USERID='foundID'
```

Flows: User Matching

- If the user has no existing account the applications user creation process is used to create a new local user.
- The unique identifiers and wanted attributes must then be appended to the created user:

```
INSERT INTO USERS
            (NAME,...,EAAHASH)
VALUES
            ('Muster',...,'f5bba3c6-6240-4ccf-8048-13dbb3405192')
```

Attributes

- Attributes are a vital part of the description of a user. They allow to identify a user and to find associated data of a user.
- Attributes are used to uniquely identify users but also to enrich an application with further information about a user.
- Attributes can be inherited from other sources of trust, e.g. eduGain or ORCID.

Accessing Attributes

- All attributes of a user are registered in the context of the login module, e.g. mod_shib2 or simpleSAMLphp, used.
- They can then be accessed programmatically, if a user has signed in:

Language	Construct
PHP	$_SERVER[“mail”];
Java	httpServletRequest.getHeader(“mail”);

Attributes

- mail (urn:oid:0.9.2342.19200300.100.1.3)
  - Preferred address for the "To:" field of e-mail to be sent to this person
- givenName (urn:oid:2.5.4.42)
  - Given name of a person
- sn (urn:oid:2.5.4.4)
  - Surname or family name

PAUL SCHERRER INSTITUT

Attributes

- eduPersonPrincipalName
  - A scoped and unique identifier of a person

- eduPersonScopedAffiliation
  - Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc.

- displayName
  - The name(s) that should appear in white-pages-like applications

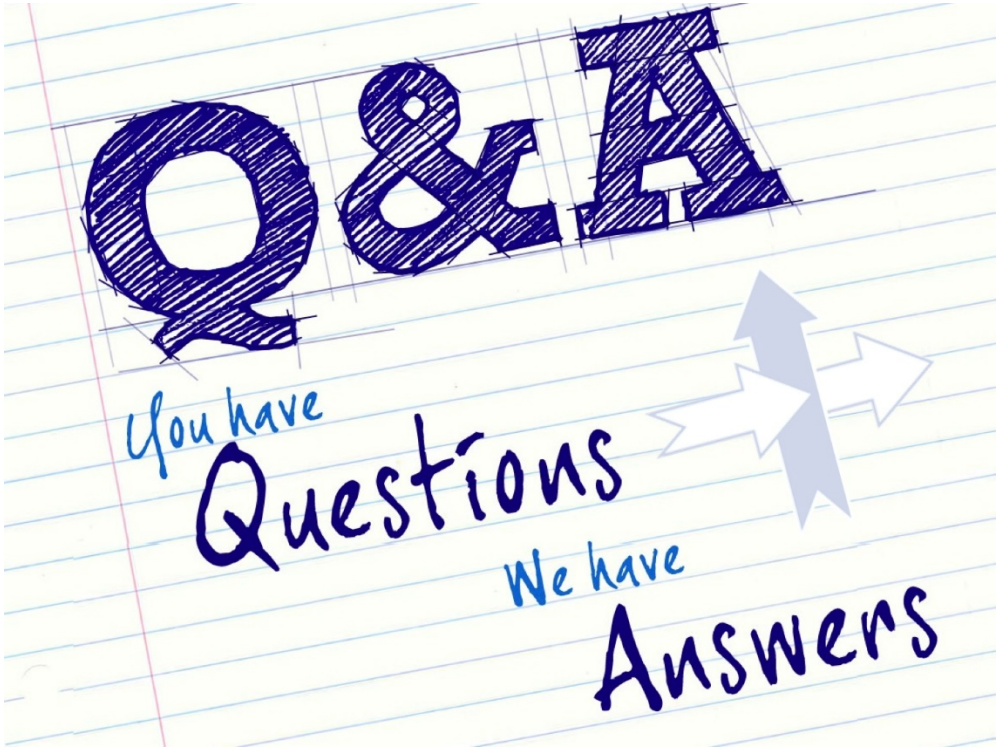
Attributes

- EAAHash (urn:oid:1.3.6.1.4.1.42750.1.1.1)
  - The unique umbrellaID identifier.

- uid (urn:oid:0.9.2342.19200300.100.1.1)
  - A unique identifier for a person, mainly used for user identification within the user's home organization

- eduPersonOrcid
  - ORCID iDs are persistent digital identifiers for individual researchers

Questions & Answers



Thank you very much!