EAA / WUO Integration

Björn Abt
PSI Villigen

Introduction

- A key feature of the EAA system is to uniquely identify a user EU-wide
- At the moment this is not possible, because all facilitites have an own user database
- The goal is to identify the user just once and use this identity on subsequent visits to different facilities and still allow existing users who don't participate at EAA to use the WUOs (hybrid aspect)

Digital ID Card

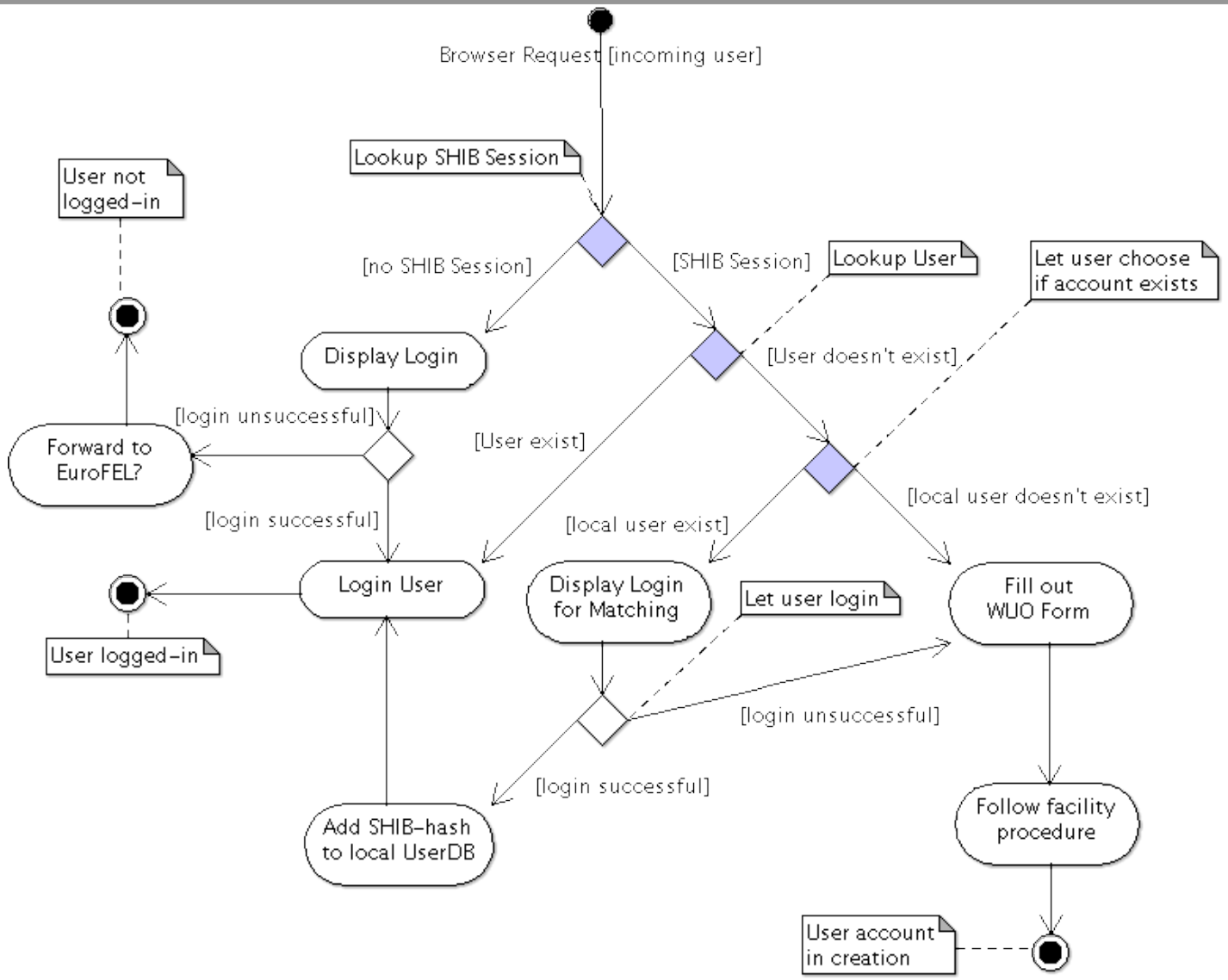
- To virtually “travel” from facility to facility a Digital ID Card is issued and used to identify the user at a facility:

Digital ID Card	
uid	**hans.meiser**
email	**6197d4e172af0c60b42b53d56206596d102392e9**
EAAHash	**c19fab6e-06db-41bb-9204-0b798a51da55**
EAABirthdate	**c21235398168063f5d4444656665fae6cc9d3872**

Implementation Recipe

- To be able to participate at EAA a WUO must install a SAML2 Service Provider software, e.g. mod_shib2.
- To be able to use the WUO software without a EAA-Session we must use the passive authentication mechanism of SAML2.
- To enable the hybrid characteristics to authenticate against WUO and EAA a multi-phase check must be implemented at the WUO

Implementation Recipe



EAA-Session Check

- Check if there is an existing EAA-Session active.
- If there is no valid EAA-Session, continue with normal application code.
- Else forward the user to the UserCheck

User Check

- Query the database for the incoming EAA-Hash.
- If there is a matching user, log him in.
- Else forward to User Matching.

User Matching

- Let the user choose to match his EAA-Account with an existing WUO-Account.
- Let the user create a new account.

DUO EAA-Session Check

- To find out if the user has a EAA-Session, a passive login request to EAA is made.
- A cookie is set to prevent further authentication checks.
- Switch provided code to implement this.

DUO User Check

- The User Check consists of an extension to the SQL SELECT statement which is used to query username and password.

```
SELECT USERNAME FROM USERS
WHERE
(USERNAME='user' AND PASSWORD='SHA1(changeit)')
OR
(EAAHASH='f5bba3c6-6240-4ccf-8048-13dbb3405192')
```

DUO User Matching

- User Matching is necessary if there is an incoming EAA-Session but no WUO user registered with it.
- Use existing “Login” and “Create User” procedures.

- If the use already has an existing account at the WUO, then a WUO login must be performed and the USERS table is updated:

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

DUO User Matching

- If the user has no existing account an account must be created and matched to the EAA-Account

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

Thank You

Thank you for your attention!

Björn Abt, PSI Villigen