Whats new @ WAYF - TNC19 - Tallin

Mads Freek Petersen, Mikkel Hald
• mEdit
  - A hierarchy-tabular schema driven metadata editor

• mRules
  - Ian’s rules for the rest of us

• MDQ
  - Issues and challenges

• jwt2SAML / SAML2jwt
  - SAML for the rest of us

• Grand Unified IdP
  - An “SP”-specific IdP

• Attribute value filtering
  - Nobody wanted to play - so we did our own …
WAYF

• Unus pro omnibus, omnes pro uno

• WAYF is responsible for - most of - the metadata

• The hybrid formerly known as a hub and spoke …

• Tags for sub-federations
  - entities only allowed to “talk” if intersection of sub-feds tags is not empty
  - enforced by hub

• Operational metadata is distributed as a SQLite db
  - compressed, signed per entity
  - lookup up by @Location or @EntityID
  - MDQ via WAYF’s ha-hub servers
  - includes FTS for discovery
mEdit
A schema driven hierarchy-tabular metadata editor

- The UI part of WAYF metadata repository
  - a plain old git repo

- Allow entities to edit selected parts of md

  - admin role - per domain - admin@dtu.dk
    entities have a organisational domain

  - Metadata tsar has root@*
the schema

'KeyDescriptor:#:X509Certificate' => [ 'xpath' => '/md:KeyDescriptor[#]/ds:KeyInfo/ds:X509Data/ ds:X509Certificate', 'roles' => ['SP/','IDP/'], 'rw' => ['admin'], 'help' => 'A base64-encoded X.509 structure containing a public RSA key, to be used for encrypting traffic to your entity and for validating signatures issued by it. Only the public key itself is interpreted by WAYF; all other content in the X.509 structure is ignored.', ],

'AttributeConsumingService:#:RequestedAttribute:#:Name' => [ 'xpath' => '/md:AttributeConsumingService[#]/md:RequestedAttribute[#]/ @Name', 'roles' => ['SP/'], 'datalist' => 'attrname', 'check' => 'datalist'
],
Ian’s “Business” Rules with our paths

• **Noes**
  ```xml
  md:EntityDescriptor[contains(@entityID, ' ')]
  ```

• **Newnoes**
  ```xml
  count(./md:Extensions/wayf:wayf/wayf:wayf_schacHomeOrganization) != 1
  ```

• **PairEqualsWithLang**
  ```xml
  .//md:AttributeConsumingService/md:ServiceName, .//mdui:DisplayName
  ```

• **Distinct**
  ```xml
  ./md:AssertionConsumerService/@index
  ```

• **ValidLocationUrl**
  ```xml
  ./@Location
  ```

• **CheckAgainstList**
  ```xml
  .//md:RegAtt’, [@FriendlyName, @Name], meditdatalists::NameFriendlyName
  ```

  ---

• **ValidCertificate**
  ```xml
  ./ds:X509Certificate
  ```

• **ValidLogo**
  ```xml
  ./mdui:Logo
  ```
To enforce sub-federation separation we must let the response depend on who asks!
- for entities that don’t have a “native” enforcement method

Combined with 4 different metadata sets
internal, hub, external-sp, external-idp

https://wayf.wayf.dk/MDQ/sp/sp.entity.test/idp.entity.test

https://wayf.wayf.dk/MDQ/sp/03e756cf22/idp.entity.test
MDQ 2

- How to send a “full” metadata set with resigned and compressed entities?
SAML2jwt / jwt2SAML

• Microservices for Service and Identity Providers resp.

• Takes care of everything SAML

• A locally run configuration less daemon

• Needs access to private key(s) and schema definitions

• Allow for very simple SPs and IdPs

• Built using WAYF’s go xml and saml libraries
Grand Unified IdP
aka
Guest User IdP
The Problem:

• Guest logins at a “SP” need be handled in a special way
  - i.e. doing identity validation and store credentials

• For the guests it is yet another username/password to remember
The Grand Unified IdP

- Outsources the authentication to a back-end IdP
  - only gets a pairwise-id
  - only 2FA accepted - e.g. UnitedID
- Lets the “SP” handle the actual identity proofing and provision the GUIdP with the necessary attributes - using LDAP/SCIM
- Lets the “SP” exchange a “SP”-specific userid for a token that is delivered to the user - in a way that satisfies the “SP”'s validation requirements
- The user logs into the GUIdP and establishes a connection btw. the “SP”-specific userid and the pairwise-id
- The “SP” can now use federated login for all users
- The user have SSO to the SP and other participating “SP”s
But What if?

- A few other SPs trusted the “SP”s user management mutually?
  - We might call that an audience

- More than a few?
  - We might call that a virtual organisation

- It satisfies a federation’s requirements
  - We might call it an Identity Provider (using WAYF’s virtual IdP service)

- The “SP” is actually a scalable attribute authority?
Attribute Value Filtering

• We need it for “internal” systems

• Tried to start a discussion on the lists
  - not an issue for others - supposedly

• We have 4 “types” of values:
  1. Prefix
  2. Postfix
  3. Wildcard
  4. Regexp
<table>
<thead>
<tr>
<th>FriendlyName</th>
<th>eduPersonEntitlement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>urn:oid:1.3.6.1.4.1.5923.1.1.1.7</td>
</tr>
<tr>
<td>NameFormat</td>
<td>urn:oasis:names:tc:SAML:2.0:attrname-format:uri</td>
</tr>
<tr>
<td>isRequired</td>
<td>true</td>
</tr>
<tr>
<td>AttributeValue</td>
<td>0</td>
</tr>
<tr>
<td>type</td>
<td>prefix</td>
</tr>
<tr>
<td>tag:entity.test:</td>
<td></td>
</tr>
</tbody>
</table>