T&I Lightning Talks
TechX 2017
Talks

- Of BetrAAIal the federated login and its salvation -
  - Renato Furter, SWITCH,
- OTTO -
  - Mike Schwartz, GLUU
- Anyroam, eduroam in the US -
  - Philippe Hanset
- Provisioning/Deprovisioning and access control using the Adaptive Object Framework,
  - Jill Gemmill, Clemson,
- User-selected authN subflows in IDIC -
  - Allan Kim, UC San Diego,
- GDPR in a nutshell –
  - Ken Klingenstein, Internet2
Of BetrAAl the federated login and its salvation
Kantara OTTO
Open Trust Taxonomy for federation Operators

Internet2 TechX Lightening Talk 2017
Michael Schwartz
Co-Chair, Kantara OTTO WG

Tweet comments @gluufederation
What problem does OTTO Solve?

- **Leverage** existing trust model to support OAuth protocols
- **Reduce** data duplication for inter-federation
- **Extend** metadata search capabilities
- **Define** common data model for federation stuff
- **Standardize** API’s for communicating with a federation
- **Support** SAML, OpenID, UMA… and _____ in the future
- **Enable** simple, extensible, open and interoperable federation!
We talked to a lot of federation experts...

- **Leif Johansson** federation security guru, “The biggest problem is not that we haven't deployed MDQ. The biggest problem is the aggregator-aggregator communication is too slow, too cumbersome, doesn't scale well. Need an asynchronous update mechanism... the problem of who talks to who, and how and what are the data types are incidental.”

- **Ian Young** co-author of MDQ “Exchanging metadata is analogous to DNS v. hosts files. But DNS is small--just an IP address--whereas the average SAML IDP metadata is 7k, and some may contain multiple certificates.”

- **Roland Hedberg** co-author OpenID Connect federation, “One of the unique approaches of this federation draft is the use of "metadata statements", which include information about a federation participant, and the services it offers.”

- **Rhys Smith** JISC Federation API developer “Automation is needed by a larger federation, and especially by participants who manage many entities. If a participant needs to update 300 certificates, it can be a challenge for both the member and the federation. An automated process to perform this task would be been more accurate and less expensive.”
OTTO Federation Actors

Registration Authority (RA)
- Hosts multiple federations.
- Hosts database, web infrastructure and performs key management (HSM) for Federation Operators
- Could be an ISP or other specialized trusted operator.

Federation Operator (FO)
- Provides governance.
- Defines the policies, procedures, schema.
- Vets participants.
- Provides first level support.

Participant
- Organization that executes the participant agreement.
- Admin and security contacts.

Entity
- Registers services
- Aligns with federation guidelines
- Management of service keys
API Endpoints

- /configuration *
- /federation **
- /participant
- /entity
- /metadata

* https://example.com/path/.well-known/otto-configuration
** The federation endpoint is where searching happens
JSON-LD Vocabulary

CORE
- Registration Authority
- Federation
- Participant
- Entity
- Schema
- Metadata

OpenID
- OpenID Provider
- OpenID RP
- User Claim
- Scope
- Metadata Statement
- Categories

SAML
- SAML Entity
- SSO Endpoint
- SSO Extension
- Service Provider
- Identity Provider
- Attribute Authority

```json
{
  "@id": "openid:OpenIDProvider",
  "@type": "rdfs:Class",
  "rdfs:subClassOf": 
      {
        "@id": "otto:Entity"
      }
}
```
First implementations?

- **First Responder?** ERASMUS Pilot – DHS Identity S&T Group  The emergency responder community is very decentralized, with thousands of federal, state, and local organizations. The OTTO federation API’s will be used to publish public keys for participants, and federation data standards for this next generation OpenID Connect federation.

- **Banking?** PSD2 Banking Federation  New banking regulations in Europe are creating standard API’s to get your balance, or to wire money. The “FAPI” OpenID Connect profile has been adopted. There is a need to create a federation between banks and payment partners to publish keys and other metadata.
Flash News.... WPA2 broken

Krackattacks.com
Turn off 802.11r as first measure
Patch Infrastructure & Devices ASAP
Unpatched infrastructure is open
Unpatched devices have no encryption
Sign Up for eduroam

Choose one of these three options:

Sign the eduroam Connector Agreement

The eduroam Connector Agreement (legal agreement to use eduroam in the U.S.) is available to sign via Docusign. A PDF review copy is available here.

OR

Sign Up for a 45-Day Evaluation

Please note: please complete this evaluation only if you are with your institution's IT staff (this is not for individual users).

Click through and acknowledge the eduroam Evaluation Terms of Use.

Don't forget to come back to sign the eduroam Connector Agreement before your 45-day trial period ends.

OR

Service Provider Only

If you want to provide eduroam to your guests, but not to your own users, you can sign up as a "Service Provider Only." For this option, contact ANYROAM directly.
Daily USA Users

- 2012: Low
- 2013: Very low
- 2014: Moderate increase
- 2015: Significant increase
- 2016: Much greater increase
- 2017: Exponential increase
This week your institution sent over 320,815 authentication requests, and hosted 3,060 devices authenticated over eduroam.

Number of unique devices authenticated over time

Accepted/Rejected requests:
- 320,815 Total number of requests
  - 213,622 Accepted
  - 107,193 Rejected

Authenticated visitors' origin

Responses to the requests:
This week your institution authenticated **1,689 devices** using eduroam hotspots.

Number of unique devices authenticated over time:

- **1,689** unique devices authenticated.
- Total number of requests: **80,589**
  - Accepted: **41,176**
  - Rejected: **39,413**

Where your users are roaming:

*Answers to the requests*
This week your institution sent over 33,520 authentication requests, and hosted 1,128 devices authenticated over eduroam.

Number of unique devices authenticated over time

- Total number of requests: 33,520
- Accepted: 19,431
- Rejected: 14,089

Authenticated visitors’ origin

Responses to the requests

October 5th - October 12th 2017
This week your institution authenticated **94 devices** using eduroam hotspots.
cat.eduroam.org (free tool)

• MS Windows 10, 8, 7, Vista - Chrome OS - iOS - MAC OS 10.7+ - Android 4.3+ - Linux
• Locks RADIUS Certificate to prevent MiTM
• anonymous@domain (privacy + automation)
• In the cloud
• Non-eduroam profiles as well
• Reduces Help Desk visits
Between local, state, and federal government

Same ease of use and security as eduroam

Contact support@anyroam.net for info
Non-edu guests on eduroam SSID
ANYROAM is a centralized IDP for guests
One registration, good for a long time
Phone number is the authenticator
Roaming Communities
Inter-Roaming Communities
Passpoint/HotSpot 2.0

Wi-Fi Access-Point advertises communities

Negotiation between AP and Device

Amount of domains for eduroam is a problem

Routing for National Roaming Operator (NRO) is a problem
Thank you

Philippe Hanset
phanset@anyroam.net
www.anyroam.net
Context Juggling

Handling user-selected authentication flows in an IDIC universe
Infinite diversity, infinite combinations

- Basis of Vulcan philosophy (ST:TOS)
- When applied to authN / authZ, arguably illogical
The original problem

- Superset of the multi-context broker problem
- UC San Diego SSO originally ran on top of multiple authentication systems (MIT Kerberos, Active Directory, IBM RACF, etc.) for distinct user populations
- Slowly consolidating systems (AD) but still need the idea of authentication as student, faculty/staff, applicant, alum, none of the above
- Add MFA to the list and generate more permutations
- Don’t even ask about OIDC / social login or we’ll cry
The solution (?)

- Define multiple local authentication flows (student, faculty/staff, applicant, etc.)
- Map flows to local authnContextClassRefs (e.g. urn:mace:ucsd.edu:sso:ad)
- Campus SP operators can request one or more authnContextClassRefs, set up matching authN/authZ rules (sometimes forget the authZ part)
- Thankfully Shib 3 moved in this direction as well!
- Auth flows for legacy / federated SPs are managed centrally – in Shib 3, injected into the AuthenticationContext with an activeFlowResolver
Visualize this!
How to handle multiple available flows?

- Extend login.vm to provide menu of available flows
- User selection handled as a SWF event
- Event ID passed to existing AuthenticationContext.signaledFlowId
- Breaks out of current authentication (sub)flow, calls the user-selected flow
How does this work with MFA in general?

- Usable (but not optimal) when MFA is implemented as part of the authentication flow (e.g. classic Duo flow)
- In theory, might work better with MFA as a post-authentication intercept flow
- Work in progress: Headless MFA for ECP (push only via Duo API)
What about the Shib 3.3.x MFA flow?

- “We’re working on that … we’ll tell you about it next year!”
- Seriously though, can adapt the existing flow mapping and resolution into a custom `nextFlowStrategyMap`
Ferengi Rules of Authentication

- Once you leak your credentials, you never get them back
- Static metadata is eternal
- A context is a context is a context
General Data Protection Regulation (GDPR)
GDPR

• The problem set and resulting requirements
• The Scalable Consent work
• The CAR architecture – a brief look under the hood and at the two user UX
• Unexpected outcomes
• CAR Management capabilities – how it performs
• Demos
  – Intercept UI
  – Self-service UI
• The Duke experience
• Next steps
GDPR (General Data Protection Regulation)

• Created by EU to manage data protection uniformly across the EU
  – Is binding for every member EU nation
  – With many global impacts
• Covers a vast waterfront of issues from tracking to attribute release to right to be forgotten to data breaches to . . .
• Consists of a set of rules (Articles) and then example interpretations of the rules in key areas (Recitations)
• Penalties of up to 4% of global revenue
• Identifies six reasons for attribute release, including contract, consent, national security, legal actions, etc.
  – Specifies when consent is not to be used, when it should be used, the quality of the consent, etc.
• It affects many, perhaps most, US institutions.
### Draft JISC Service Categories

<table>
<thead>
<tr>
<th>Risk level</th>
<th>Relationships</th>
<th>Current example</th>
<th>T&amp;C template</th>
<th>Privacy notice template</th>
<th>Legal basis test</th>
<th>DP Impact Assessment?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>People using this service have direct interactions with Jisc (e.g. read a website, ask for information)</td>
<td>Jisc website, Jisc Collections website, Jisc Archives Hub Helpdesk</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>People using this service have a direct, long-term relationship with Jisc (e.g. hosting a registered local admin)</td>
<td>Mailing lists, Calafi for Participants, Purchasing Frameworks</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>Service with remotely administered users (e.g. managed by third parties). Jisc relies on 3rd party to communicate to users</td>
<td>Edrooom, Online Surveys, Research Data Store</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>4</td>
<td>Service where we have no relationship with the users at all; they may be unaware it exists</td>
<td>Learning analytics, Security Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

» Guide to priorities and which template/model to start from
» And how much effort to allow for adapting them
Some gnarly details

- PII and Sensitive PII
  - Almost everything is PII – from IP address to persistent identifiers
    - Some identifiers are not e.g. ePTID
  - Sensitive PII
    - Religious, ethnic, sexual, health, trade-union membership, etc.
    - Requires special handling in everything from protection to presentation
- Research data use
- Right to be forgotten
  - Cloud based backups
- “This call may be recorded...”
- Data breach notifications
  - 72 hours
- Data protection officer and individual data protection training
Consent and GDPR

- GDPR is specific on when to not use and to use consent, and the nature of consent when used
- For many university core services, “legitimate interests” may be used to avoid the use of explicit consent
- Some institutions feel a consistency of experience and transparency are important
- A consistency of consent experiences across devices and providers is desirable
- The quality of the consent is very important
  - Distinct experience
  - Revocable
  - Informed
  - Fine grain – data minimization
  - Handle sensitive values
- Users seem to get it
Resources

- AACRAO - http://www.aacrao.org/resources/trending-topics/gdpr
- Solove
- Andrew Cormack blogs – e.g. https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-whats-your-justification
- Characteristics of GDPR compliant consent -