European Workshop on Trust & Identity

Connecting Identity Management Initiatives

EWTI 2014 Session Notes – Table of Contents

This document contains the proceedings of the EWTI open space held on December 3.-4., 2014 in Vienna, Austria.

1 IdP of Last Resort (home for the homeless, UnitedID.org)

Convener: SteveO
Main scribe: Licia
# of attendees: ± 20

Main issues discussed: The session focused on use-cases and possible architectures to implement IdPs of last resorts.

Why - to support people affiliated with an organisation without an IdP or people that change institution frequently (i.e. contractors, researchers, and so on). Scott K noted that EU IdPs are not releasing attributes to US – this could be a good use to look for the homeless IdPs.

What options – There is of course the option to use social IdPs (i.e. Google, Facebook and the likes). Privacy concerns aside, these IdPs cannot assert eduPerson attributes, which are required by many services in the R&E community. PayPal was also mentioned as a more trustworthy IdP, which would also provide a stronger user vetting. The discussion covers different options such as:

UnitedID is an IdP based in Sweden, with premises in the US. It's a SAML based IdP two-factor based. The difference between UnitedId and Google is that UnitedId promised to handle user-data in moral way. It also offers a step-up level of assurance. Discussion is on-going to use PayPal to elevate the identity verifications. This could be included in future releases of UnitedId. It also supports consent. The business model is still under development; at the moment users do not pay, but eventually RPs may be charged.

IdP in the clouds like the solution offered by GARR

Social IdPs they can be used for contractors that are still affiliated with the Universities. Social accounts could be connected to an Attribute Providers to elevate the identity. Main problem with Facebook is that when a RP asks for some information, then the users has a binary choice (either to allow the RP to get everything or no access). Peter Gietz proposed a model to address this aspect by linking the IdPs authN with something like Protected Network to get the persistent identifiers. However the user experience may be hindered.

Austrian government approach – A solution was presented to show the system used by the chamber of commerce (which operates their own federation). The user that wants to access an relaying party is sent to the chamber of commerce IdP to login. They do account linking with the government system (based on social security number).

Q: Should we have a EU last resort IdP? –
A: The risk related to this should be assessed, as this IdP could be massive in size; legal implications of keeping data should also be covered.
Furthermore some services may have trust issues with an IdP they don't know.

Insights / action items / next steps: No concrete steps; it was noted that if the AARC project will be funded, some of the work in this area will be addressed there.

2 Auth Bridge between STORK and eduGAIN

Convener: Enrico Venuti
Main scribe: Rainer
Slides: here

Main issues discussed:

Explaining STORK infrastructure, availability in member states
Think of connected Hub-and-spoke federations per member state
Q: What is the link between the affiliation o a university and the citizen id? A: Government may leverage student ids for government services - e.g. if governmernt eIDs are lacking.
The use case under discussion is the use of STORK eIDs for SPs. Could be bootstrapping citizens into academic world, research collaborations, guest IDP, high level assurance.
STORK use cases are student mobility, ECAS (access to European commission services), change address)
STORK 2 will be move to e-SENSE for long term operation, to be integrated in the Connecting Europe Facility

People make an assumption, that any ID in STORK is only an academic ID; e.g. CLARIN is requiring this. eduGAIN cannot filter out non-academic IdPs.
FutureID is working with swarms of identity brokers that may have different policies. The proxies are data controllers, decrypting/re-encrypting/re-signing assertions. Governance is like CAs.

There is a project in STORK to interface with GRNET. There are technical and political issues, and there are disconnected discussions in several communities. Technical issues have been examined and can be resolved in gateways on both metadata and protocol level. There will be a release of a gateway as OSS in early 2015. There are pee-to-peer pilots in countries. Metadata is not yet dynamic.

What to do with non-EU federations?
Will STORK-SAML be evolving - rather not, but a gateway can speak SAML2int to eduGAIN.

This session was merged with the proposed session “Top 3 reasons to abandon STORK for eduGAIN”.

3 Government ID for Research & Education a.k.a. Separating AuthN and AuthZ

Convener: Niels van Dijk (SURFnet), Manne Miettinen (CSC)
Main scribe: Lukas Hämmerle
# of attendees: ~20

Main issues discussed:

* In the Netherlands government launches new ID system
  - Interesting for higher education federations to verify identities using that ID
  - Could be used as alternative or to improve Guest identities, which have a very poor assurance level due to self-registration
* In Finland the government is starting to build a national authentication solution where the user can choose what strong authentication tokens (mobile, bank, smart card, etc) he/she wants to use
  - Currently there are two identity federations in Finland (Haka and Virtu) where the IdPs take care of both authN and authZ
  - one can envision a future where the role of the current identity federations is only to provide attributes of the users that are authenticated elsewhere
  - pressure to decouple authN and authZ arises also when users want to use their Facebook or Google id fo authN but get their attributes related to studentness from the University registers
  - the key connecting the identities could be the personal identity number or its 21st century version “electronic access identifier” stored in the population information system run by the Population Registration Centre (a government office)
  - personal identity number discloses the birth date and sex of the person, electronic access identifier is only a unique identifier
* In Denmark every person has a unique CPR (central person registry) number, which is considered an authenticator
  - Banks and public sector are allowed to use CPR number with NemID and Nemlogin
  - WAYF.dk is allowed to use Nemlogin/NemID, but in other countries like the Netherland and Switzerland this would not be allowed
  - In Denmark universities now CPR number in advance, which is then for example also used for password reset
  - CPR in Denmark contains birthday
  - NemID is PKI-based solution where private key is stored centrally (contract with company ends soon)
  - Tax records are public in Denmark

* In Sweden, the person identification number is not considered sensitive data,
  - 12 characters including gender and birthday
  - Everybody can access open registry (run by taxation department) with this person number, which contains name and adress
  - Authoritative postal mailbox address is stored in registry
  - One problem is for example that foreigners (about 20% of all students) don't have an ID. This problem led to eduID.se.
  - Registry and authoritative mailbox are used in SWAMID eduid.se to verify identity by sending a "token" to mailbox (-> Upgrade to Assurance Level 2)
  - Foreign students get another person number (containing birthday and gender) for use within university eco system
  - Tax records are public in Sweden too
  - Any person can look up persons in that database
  - Name and address are considered sensitive data
  - Campus services often need more attributes than an identifier, therefore SWAMID intends to run a proxy that aggregates and enriches attributes
  - Authentication comes from eduID
* In Switzerland a person identifier exists with main purpose for retirement/social security/health insurance
  - Very restricted usage policy, even government cannot use that number in some cases
  - Identifier is considered sensitive data, 13 digit number
  - Swisscom (largest telecom company) intended to run a broker service for identities but cancelled the project because it was considered too risky

Insights / action items / next steps:

* Private company can hardly create national infrastructure, it should rather be the government
* Personal identifiers are widely used in Scandinavian countries.
  - Some of them contain personal information like birthday and gender
  - Usage (identifier vs authenticator) varies from country to country
* In other countries like The Netherlands and Switzerland personal identifiers also exist but usage is much more restricted, mostly due to data privacy laws

Additional information regarding official Swiss e-government (e-society) standards for electronic identities and federated identity and access management below. Standards etc. are currently available in German and French. If you need further information, don’t hesitate to contact thomas.selzam@bfh.ch.

- **eCH-0107 Design principles for IAM V2.0**
  - eCH-0107 defines principles, rules and a regulatory framework for the design of IAM systems for the provision of federated IAM solutions in the sector of the federal e-government in Switzerland. The design principles define an exemplary IAM landscape in cross-organisational application scenarios for existing and future applications, under the general assumption that the business services can be used and provided by different stakeholders. This standard specifies requirements, stakeholders, processes, information architectures, business services, and potential identity federation models. This standard is applicable to any area of the e-society.
- **eCH-0167 SuisseTrustIAM framework concept V1.0**
  - SuisseTrustIAM is a concept for a generic identity & access management solution for e-government, e-health, e-education, and e-economy. SuisseTrustIAM defines a generic platform that enables easy connecting of solution providers and data providers, of providers and consumers of identity information. At core of it lies a broker infrastructure, which enables authentication of subjects (represented through an electronic identities) and qualified verification of attributes belonging to the same subjects, through registers or directories of companies or organisations, including traceability. This document contains the global concept of SuisseTrustIAM, describing its core functionalities and components. It provides a basis for technical, organisational, and semantic specifications and it serves as a model to deviate use cases, requirement and communication protocols.
- **eCH-0168 SuisseTrustIAM technical architecture and processes V1.0**
  - eCH-0168 describes potential, technical implementations and core processes required to implement a solution following the eCH-0167 standard.
- **eCH-0169 SuisseTrustIAM business architectures V1.0**
  - The Standard eCH-0169 describes the business architecture of SuisseTrustIAM (see eCH-0167). It describes from a business perspective the stakeholders, roles, tasks, and processes in the context of SuisseTrustIAM. It also focusses on aspects of governance, and management of SuisseTrustIAM. Governance and the management are understood as tasks that are to be kept separated. This is further reflected in the definition of two separate, organisational structures (boards). These are tasked with the coordination of all stakeholders within a domain, enabling them to establish trust within

their domain. The governance board defines policies and supervises the compliance with those, while the management board implements the policies among the stakeholders and monitors the implementation. A federated identity and access management such as SuisseTrustIAM is a very important component for integrated e-government, e-health, e-education, and e-economy.

- **eCH-0170 Quality model for electronic identities V1.0**
    - eCH-0170 defines the core aspects of electronic identities with regards to quality.
- **eCH-0171 Quality model for attribute providing V1.0**
    - eCH-0171 is used for the evaluation of the quality of attribute assertions. It describes the basic processes for providing attribute assertions and derives therefrom quality criteria for the evaluation. Through the definition of possible quality characteristics are defined and enable an easy evaluation of the attribute assertion. The quality model allows the comparison of different attribute assertion providers.
- **eCH-0172 IAM maturity model V1.0**
    - The IAM maturity model helps organisations to identify the state of their IAM implementation. An organisation can monitor the development of their IAM maturity and compare itself with the best practices within the industry. It allows demonstrating the value of the IAM in order to show the advantages of an IAM strategy and the state of implementation of the strategy. This also facilitates meeting the requirements of governance, risk and compliance (GRC).

The Netherlands

- Restrictions on use of personal identifiers (BSN), may only be used for “government business”
- Two active separate systems DigID (G2C) and eHerkenning (G2B)
- DigID: Government to consumer
  - Uses SAML 2 now, releases BSN. U/P auth with SMS for higher LoA.
  - One government run “IdP”. Registration based on sending letter to postal address in municipal registration.
  - Specs: https://www.logius.nl/fileadmin/logius/ns/diensten/digid/koppelvlakspecificaties/Koppelvlakspecificatie_SAML_DigiD4_v3.0_definitief.pdf (Dutch, sorry)
- eHerkenning (eRecognision): Government to business only:
  - Private parties offer authentication and registration services
  - Specs: https://www.eherkenning.nl/eRecognition
- New unified architecture being developed: eID
  - Open for use by private parties. Both offering authentication services and using authentication services.
  - SectorIDs (sector specific IDs). Sector can be e.g. healthcare, education
  - More information and draft specifications http://www.eid-stelsel.nl (note: very likely to change)

4 Step-up (strong) authentication as a service

Convener: Pieter van der Meulen (SURFnet)
Main scribe: Manne MIettinen (CSC)
# of attendees: 16 + convener

Main issues discussed:
SURFnet is developing SuaaS (step-up authentication as a service) in PHP
How to add step-up authentication in an existing federation (differences in hub and mesh architecture federations)
LoA 1-3
Currently LoA ievels are defined/interpreted by the operator
Biometrics has different levels of LoA, although popular perception thinks its always high
Identity assurance
Authentication assurance
SAML
OpenIDConnect
Registration process
Registration roles
User's nterest? In SURFnet around 5 institutes will start next year
Metadata management in ADFS
simpleSAMLphpLib

Insights / action items / next steps:
"Every problem can be solved by adding a proxy" ;-)
"When can we have it?" ~ The gateway will be available in 6 months as Open Source software (GItHub)
"Cool stuff"

5 Federations within Federations: Enabling Local/Ad Hoc Policy Spheres

Convener: Ann West
Main scribe: Niels
Additional scribes: Rainer
# of attendees: 12

Main issues discussed:
Use cases:

- how to add additional policy on top of exiting federation (this could be state fed's)
- different policies could pertain to privacy, news,
- Pick out specific Service provides that are suited for a group of IdPs
- Specific IdPs certificated to be able to be AuthN providers for GOV, (this is the FICAM program) Certification on LoA 1 or 2 is inserted in metadata; this is check by the government SPs. FICAM is not a federation, they have a bridge (FCCX). Internet2 does not want to enable general citizen use cases. This is outside of their policy (R&E identity federation)
- Niels: VOs are a similar scenario - federations within federations. They use a subset of IdPs and SP with CALRIN as an example that actually publishes its own metadata. Scott says that LIGO is a similar case. Niels: many of the VO policies are managed locally, and are not interesting on a general scope. Policy owners and metadata owners migth be quite different.
- Rainer: Intranets of large organizations have a similar case as VOs, using the same federation infrastructure for internal and external applications.

SPs could join different local federations - this is similar to joining eduGAIN and the NREN. It should be single technical instance, but appearing in different policy contexts. Metadata can just inherit the general policy of the group (like UCSD does), or tags could be inserted. InCommon develops a registry of all tags.
Niels: there are so many groups (like LIGO) that this would not scale distributing tags in metadata. Roland: But you need this for attribute release. Niels/Ann: it is a group management problem, that has to be solved on top of federation.
How to discover the right entities? Could be done with ECs at both SPs and IDPs. An MDX extension could be used to query for a tag.
Branding an SP with a tag would help to ease attribute release with IDPs, the tag owner would vouch for the group of SPs.
Leif has been promoting the “e-Science” tag for the group of VOs like CLARIN and LIGO. It is a bottom-up approach fro reputation building.

Mads: Would consent solve a lot of the attribute problems? Ann: the IDPs are asking to the ARP: who is vetting, is this really needed, is the service following the definitions of the entity category?

Insights / action items / next steps:

Niels proposes follow up session

6 Vectors of Trust

Convener: Steve O.
Main scribe: (Not) Brook Schofield
# of attendees: 15 (Xaver, Steve O. Wolfgang, Lukas, Slavek, Philipp, Wolf, Kari, Mikael, Marina, Brok, Jon, Peter S., xxxx, Peter G.)

Main issues discussed:

Steve referred to NIST SP 800-63 document (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf) and how it doesn't work for some of the use-cases we might be interested in.

As a result there is Vectors of Trust (VoT) - the use of the term Vectors might be replaced with "factors" or something else to better describe the goals.
https://www.ietf.org/mailman/listinfo/vot
http://www.ietf.org/mail-archive/web/vot/current/maillist.html

Specific discussion focused on the VoT strawman by Justin Richer
http://www.ietf.org/mail-archive/web/vot/current/msg00004.html

Jon referred people to the Good Practice Guides
https://gds.blog.gov.uk/2012/05/14/good-practice-guides-enabling-trusted-transactions/
Specifically GPG43
https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services
and GPG45 https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

NIST will be producing an RFI (expected in 2015) on an update to NIST SP 800-63-2. It is likely that they can only look at other Standards Defining Organisations (SDOs) to no go down this path.

7 All the cool kids are using JavaScript frameworks and ignoring SAML…

Convener: Brook Schofield
Main scribe: Brook Schofield
Additional scribes: Rainer
# of attendees: 8 (Dominic, Thomas W., Leonhard, Andre, Scott, Rainer, Mads, Brook, Tommas, Roland, Thomas)

Main issues discussed:

AT chamber of commerce (WKO) is using ADFS, internally not SAML, but WS-Fed.
All the tutorials suggest storing passwords internal to the application. The tutorials might extend further to support something like OpenIDConnect (JWT).
160 identified users - so it is easy to

Bootstrap methods for federated apps - SAML2 and OpenIDConnect - is often that you don't know the user.
Other environments my already know the user and therefore

What are the options?

- Provide SAML tutorials for their framework.
-

Three types of application:

1. Server Side Application (pages rendered on the server and sent to the server)
2. Rich JavaScript Application (everything in the browser)
3. Hybrid Application - "protected" data from the server and a Rich JavaScript interface.

The problem with apps based on single-page frameworks is that the browsers collect a lot of state before a login is required. At that time it should be avoided to redirect to another page. iframes and popups are fraught with problems, like SOP and cannot share cookies with the initial frame. You might open a new window. There is a risk of losing these application's users if there is no solution for federation.

These frameworks are not dumb web browsers any more. They should do SAML ECP etc. Javascript could solve the discovery part.

How to make SAML work with your REST API?
How to design a REST API to work with SAML?

AAF is using Rapidconnect, kind of SAML to JWT gateway, not full OIDC.
https://rapid.aaf.edu.au

Insights / action items / next steps:

- Look at writing:
    - “Non-Web Application Best Practice Authentication Guide” (original idea from Joost van Dijk)
    - “Integrating <<lang>> Applications with SAML” (our new idea)
        - <<lang>> is an enumeration of JavaScript, Node.js, Scala, Erlang, Go, ...

8 Introduction to XDI (eXtensible Data Interchange)

Convener: Markus Sabadello, André Martins
Main scribe: Markus Sabadello
Additional scribes: :
# of attendees: 7

Main issues discussed:
We gave a quick introduction of the XDI data model and architecture, which is conceptually similar to RDF and other semantic web technologies, but also has a few unique features.
We had a quick look at the historical evolution of XDI, the level of adoption, and current efforts to advance the technology.
We discussed the distributed nature of graphs, where every XDI address can potentially be a reference to additional XDI graphs in different network locations.
We discussed the role of registries and discovery. XDI graph servers are distributed, but a centralized registry may be a problem.
We had two quick demos:
1. Using a web browser, creating a permanent "data connection" between an individual's "personal cloud" and a business, and
2. A browser plugin which is like "Twitter for data", which allows individuals and organizations to "follow" each other

Insights / action items / next steps:
If interested, look at the homepage of the XDI2 open source project (http://xdi2.org), and try the "XDI Ninja!" browser plugin (http://xdi.ninja/)

9 SAML/OIDS Metadata IOP || Dynamic Metadata Exchange (GNTB)

Convener: Rainer, Daniela
Main scribe: Rainer
Additional scribes: : please help
# of attendees: 12

Main issues discussed:
Roland: Usually in OIDC a RP (=SP) will register at the IDP with name and callback URL. But there is a dynamic registration as well. An implicit concept is that domain validation can be leveraged with Webfinger. MDX or signed metadata could be used to provide signed information, but there is no profile on that currently available.
Géant Trust Broker is a kind of extended discovery service.
Requires good data metadata, otherwise

Pieter: The federation requires contractual trust, domain validated data is not replacing this.
Roland: In the previous session we were talking about VOs defining entity categories. (VOs scaling from 10 to 100k of persons). OIDC has the notion of aggregated and distributed information, as opposed to centralized SAML metadata. The OIDC provider would only sign the essential items.

GNTB tries to leverage the user's trust into the SP to get the IDP tp release data. People have reservations that IDPS would release attributes based on that data. The question is who do you trust. The federations are not something the IDPs really trust. Therefore, the R&S category is not trusted either. Rather the research organizations are trusted, more like a WoT. Even within DFN attribute release is difficult, only on bilateral basis.
GNTB is helping the user at the point of IdP discovery. This could be solved as a service outside metadata, by users vouching for an SP, with a certain mass supporting a decision at the IDP to federate and release attributes. SURFnet is already supporting such a business process for their federation. But this is easier in a H+S federation.

Insights / action items / next steps:
SAML has good support for enabling trust, OIDC has not yet defined this.

10 FIDO and something about 2 factor

Slides can be downloaded here.

Convener: Tom
Main scribe:
# of attendees: 20

Main issues discussed:

U2F Protocol (Universal Second Factor) - no client software - but software needs to be incorporated into the client. i.e. Chrome has support.
Anti-Phishing: Would be interesting to understand how this happens.
https://developers.yubico.com/U2F ← Client for C, Java, Python, PHP.
http://fidoalliance.org/adoption/fido-ready/
A cheaper alternative is http://www.buysecuritykey.com/ and supports U2F.

11 Delivering LoA using SAML AA/LoA/provenance on attribute level

Convener: NIels
Main scribe: Manne
# of attendees: 18

Main issues discussed:
Why do we not use eduPersonAssurance?

- The discussion on vectors of trust addressing questions Wolfgang has in mind
- Vector of trust idea does not mean giving one numerical value for trust; it can also mean sending all the different trust vectors for the user to be decided

How to query additional (assurance) information from a Virtual Organization?

- missed a bit this discussion...

Attribute provenance or the LoA of particular attributes

- How to get LoA of a single attribute? In LDAP there's a technical solution (attribute option) e.g. givenName; lang-en: Paul, givenName; loa-1: Niels. This solution would work for trust vector information; how to express this in SAML
- How to ship LoA info simply without inventing something new? Shibboleth or simpleSAMLphp would implement new inventions fast, some commercial vendors would be slow
- Elixir use case: 2 mechanisms for vouching a persons LoA a) admin selects b) five people vouch for a person to be member
- LoA is not only about the technical solution to express LoA it also brings a burden for the data management that comes with a price
- eduid.se expresses authentication context content class which is a different case (binary)
- STORK has mandatory LoA, but it doesn't mandate minimum level of LoA
- in eduID the person's name is self asserted
- Should not mix Provenance and Level of Assurance; especially the word "Level" causes misinterpretations; Provenance seems to be more viable approach
- TERENA meeting in Belgrad came up with well thought of attributes; these minutes will be posted to the REFEEDS list and addressed tomorrow 4.12.

Insights / action items / next steps:

- Detailed use cases is the way forward

12 SAML and/or OIDC / Multi Stakeholder Trust Building in OIDC "Federations"

Convener: Niels van Dijk, Roland Hedberg
Main scribe: Pieter van der Meulen
# of attendees: 10

Main issues discussed:
How do SAML federations currently handle metadata?

- They keep a “telephone book” with all SPs and IdPs in their federations. The list is signed by the federation operator and contains all identifying information (names, keys, endpoint addresses).
- This can become big in big federations like e.g. eduGAIN. New is a MDX, a query service for dynamically querying metadata

How does this work in OpenID connect?

- Webfinger is used dynamically for discovery. RP finds OP by webfinger address (user@domain)
- Configuration downloaded from OP (==IdP in SAML) by RP (==SP in SAML) in an unsigned JSON document
- There is no third party to provide trust in this setup

How to add trust to the OpenID connect setup?:

1) RP finds OP
- Use secure DNS (webfinger published in DNS)
- Add a third party a signature to the configuration data. The third party used JWS (signed JSON web token) to sign (part of) the JSON data.
- This way is within the way the standard currently works.
- Needs implementation by RP & OP. This is not currently there
- Mobile operators GSMA has a working group working on such a solution

2) RP registered at OP
- Trust in current standard solution relies on data received from SSL. Messages are / cannot be signed with key derived from trust.
- RP registered at OP (OAuth). It can use a secret to prove who it is.
    - Can’t run on mobile device (same with SAML SP)

13 Dashboard and portal for IdP and/or end users

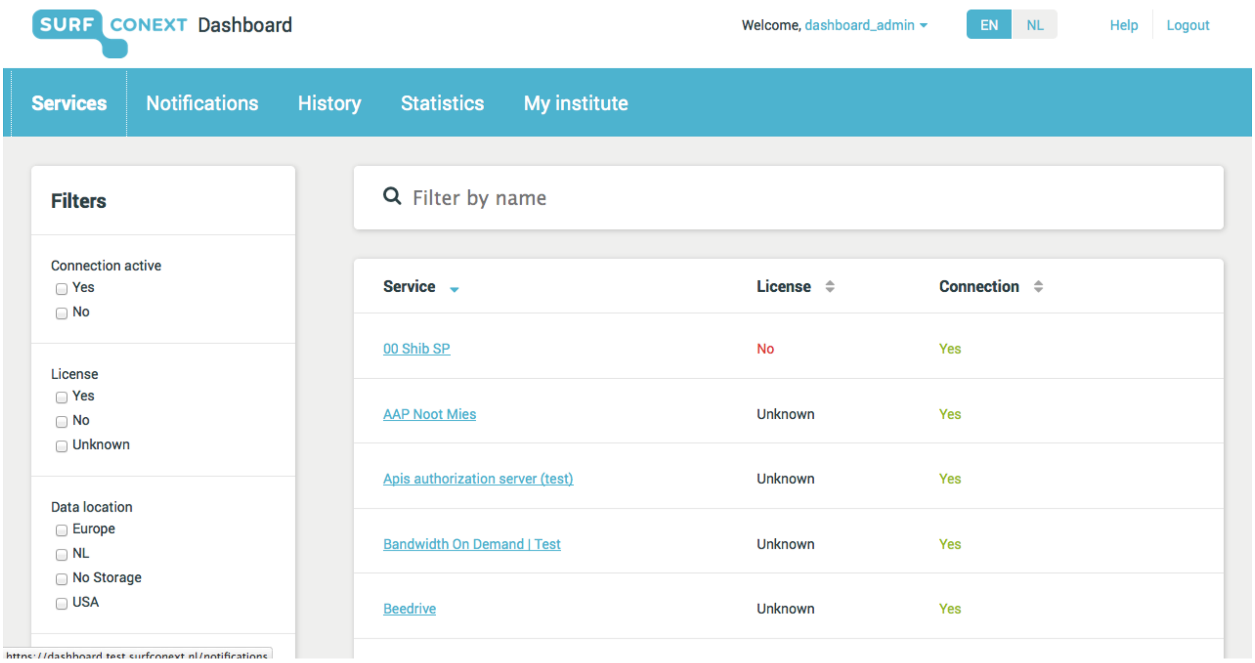
Convener: Femke Morsch

Main scribe:

# of attendees: 12

Main issues discussed:

- What should you show to end users?
  Keep it simple
  Support information (also add telephone number)
  Live Availability of the SP
- How do you get rich information from Service Providers?
  Metadata would be helpful for this, but where do you draw the line? Logo, description, support, license info, screenshots?
- Use the advantages you have as a hub and spoke - show which SPs are available for end users of a certain IdP. Make it possible for end users to log in if they want to.



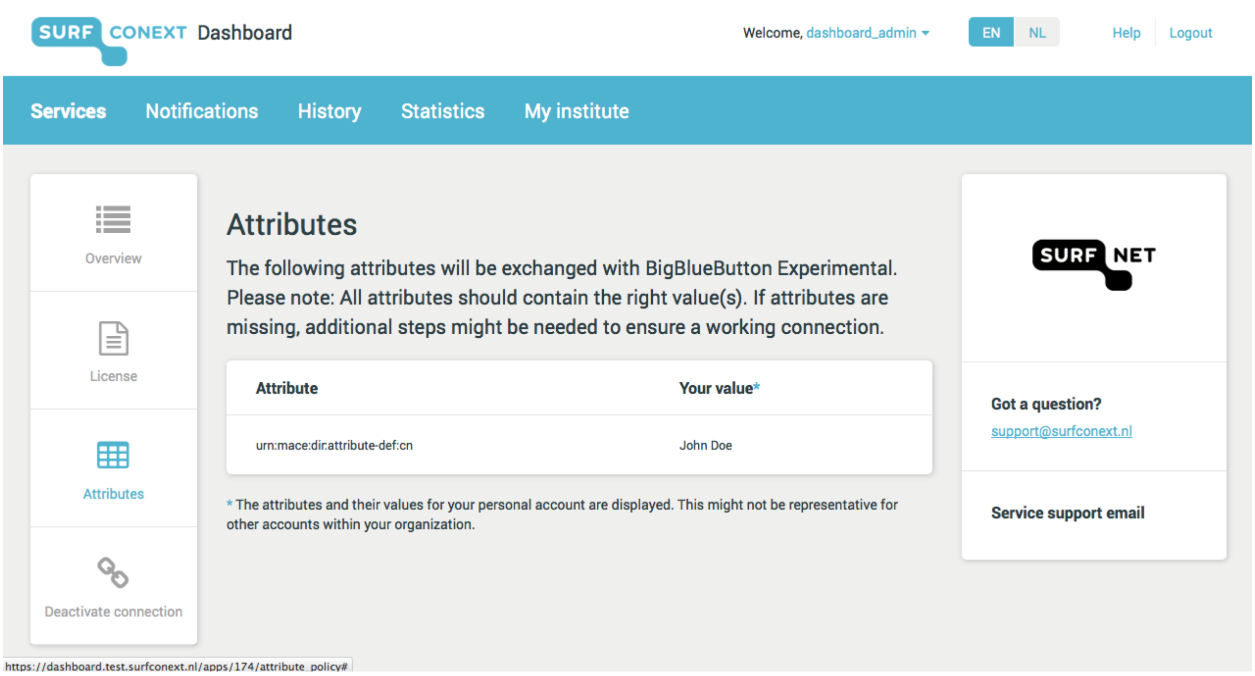
Filters

Connection active
☐ Yes
☐ No

License
☐ Yes
☐ No
☐ Unknown

Data location
☐ Europe
☐ NL
☐ No Storage
☐ USA

Service	License	Connection
00 Shib SP	No	Yes
AAP Noot Mies	Unknown	Yes
Apis authorization server (test)	Unknown	Yes
Bandwidth On Demand | Test	Unknown	Yes
Beedrive	Unknown	Yes



Attributes

The following attributes will be exchanged with BigBlueButton Experimental. Please note: All attributes should contain the right value(s). If attributes are missing, additional steps might be needed to ensure a working connection.

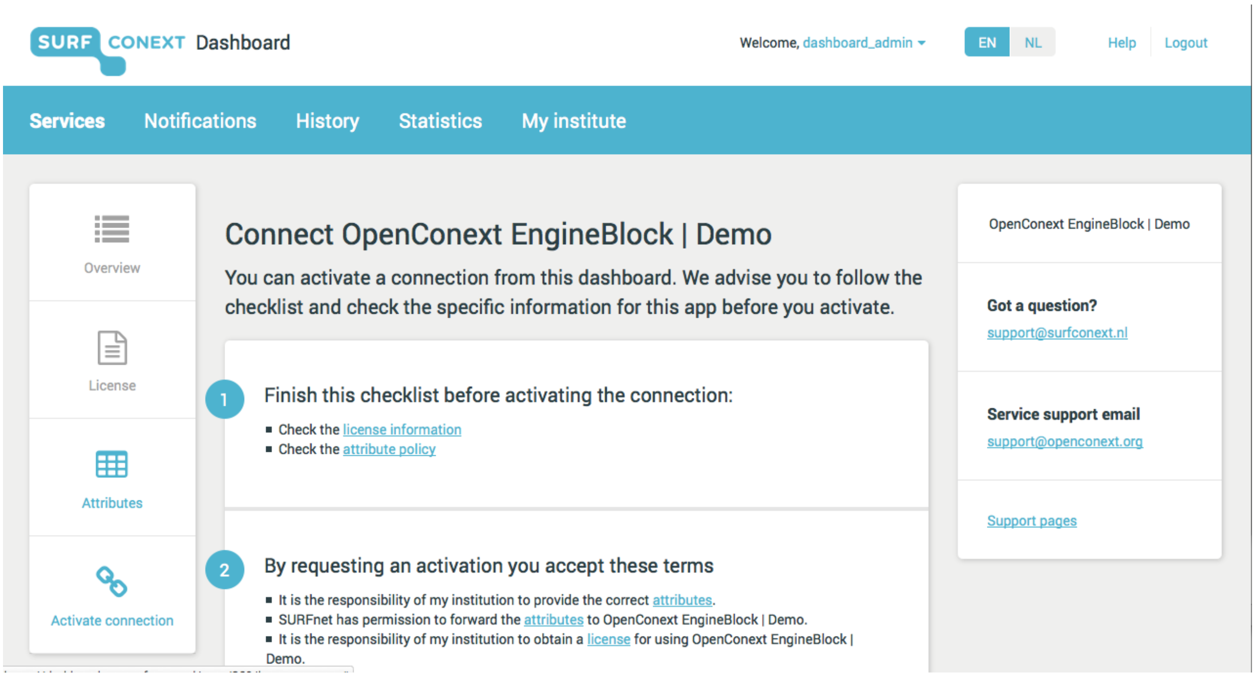
Attribute	Your value*
urn:mace:dir:attribute-def:cn	John Doe

* The attributes and their values for your personal account are displayed. This might not be representative for other accounts within your organization.

Got a question?
support@surfconext.nl

Service support email

https://dashboard.test.surfconext.nl/apps/174/attribute_policy#



Connect OpenConext EngineBlock | Demo

You can activate a connection from this dashboard. We advise you to follow the checklist and check the specific information for this app before you activate.

1 Finish this checklist before activating the connection:

- Check the license information
- Check the attribute policy

2 By requesting an activation you accept these terms

- It is the responsibility of my institution to provide the correct attributes.
- SURFnet has permission to forward the attributes to OpenConext EngineBlock | Demo.
- It is the responsibility of my institution to obtain a license for using OpenConext EngineBlock | Demo.

OpenConext EngineBlock | Demo

Got a question?
support@surfconext.nl

Service support email
support@openconext.org

Support pages

14 Delivering LoA using SAML AA

LoA/Provenance on Attribute level

Convener: NIels

Main scribe: Manne

# of attendees: 18

Main issues discussed:

Why do we not use eduPersonAssurance?

- The discussion on vectors of trust addressing questions Wolfgang has in mind
- Vector of trust idea does not mean giving one numerical value for trust; it can also mean sending all the different trust vectors for the user to be decided

How to query additional (assurance) information from a Virtual Organization?

- missed a bit this discussion...

Attribute provenance or the LoA of particular attributes

- How to get LoA of a single attribute? In LDAP there's a technical solution (attribute option) e.g. givenName; lang-en: Paul, givenName; loa-1: Niels. This solution would work for trust vector information; how to express this in SAML
- How to ship LoA info simply without inventing something new? Shibboleth or simpleSAMLphp would implement new inventions fast, some commercial vendors would be slow
- Elixir use case: 2 mechanisms for vouching a persons LoA a) admin selects b) five people vouch for a person to be member
- LoA is not only about the technical solution to express LoA it also brings a burden for the data management that comes with a price
- eduid.se expresses authentication context content class which is a different case (binary)
- STORK has mandatory LoA, but it doesn't mandate minimum level of LoA
- in eduID the person's name is self asserted
- Should not mix Provenance and Level of Assurance; especially the word "Level" causes misinterpretations; Provenance seems to be more viable approach
- TERENA meeting in Belgrade came up with well thought of attributes; these minutes will be posted to the REFEEDS list and addressed tomorrow 4.12.

Insights / action items / next steps:

- Detailed use cases is the way forward

15 All the cool kids are using JavaScript frameworks and ignoring SAML…

Convener: Brook Schofield
Main scribe: Brook Schofield
Additional scribes: Rainer
# of attendees: 8 (Dominic, Thomas W., Leonhard, Andre, Scott, Rainer, Mads, Brook, Tommas, Roland, Thomas)

Main issues discussed:

AT chamber of commerce (WKO) is using ADFS, internally not SAML, but WS-Fed. All the tutorials suggest storing passwords internal to the application. The tutorials might extend further to support something like OpenIDConnect (JWT).
160 identified users - so it is easy to

Bootstrap methods for federated apps - SAML2 and OpenIDConnect - is often that you don't know the user.
Other environments my already know the user and therefore

What are the options?

- Provide SAML tutorials for their framework.
-

Three types of application:

4. Server Side Application (pages rendered on the server and sent to the server)
5. Rich JavaScript Application (everything in the browser)
6. Hybrid Application - "protected" data from the server and a Rich JavaScript interface.

The problem with apps based on single-page frameworks is that the browsers collects a lot of state before a login is required. At that time it should be avoided to redirect to another page. iframes and popups are fraught with problems, like SOP and cannot share cookies with the initial frame. You might open a new window. There is a risk of losing these application's users if there is no solution for federation.

These frameworks are not dumb web browsers any more. They should do SAML ECP etc. Javascript could solve the discovery part.

How to make SAML work with your REST API?
How to design a REST API to work with SAML?

AAF is using Rapidconnect, kind of SAML to JWT gateway, not full OIDC.
https://rapid.aaf.edu.au

Insights / action items / next steps:

- Look at writing:
    - “Non-Web Application Best Practice Authentication Guide” (original idea from Joost van Dijk)
    - “Integrating <<lang>> Applications with SAML” (our new idea)
        - <<lang>> is an enumeration of JavaScript, Node.js, Scala, Erlang, Go, ...

16 Federations in Federations (cont)

Convener: Niels/Ann

Main scribe: Niels/Ann

Additional scribes: :

# of attendees: 10

Main issues discussed:

Three tagging areas:

1. Community based tags for tailored policy spaces. Federation does due diligence about ownership of namespace.. These are curated by community organizations.
2. Gross categories of eduGAIN members to identify basic providers
3. Well-defined set of entity categories that are international and supported. These are curated by Federations and are defined by REFEDS.

Filters vs. entity categories-

- UK Access publish SPs by default aren't germane to eduGAIN, such as New Castle-specific SPs.
- Is this service relevant for an international audience?
- Could use Hide from Discovery. (more about "not intended to be used" as opposed to not relevant)
- If we're jus applying generic not-vetted labels, it could be very confusing regarding the intent behind the tags.

If we can get some base tagging adopted, we'll need tools to help the have-nots Shouldn't we get R&S going first and not distract ourselves from adding this new approach? Do community tags have enough value? Should we work from the top down (broad entity categories like R&S) AND bottom up (specific VO tags).

17 How to provision users after SPML and SCIM?

Convener: Rainer Hörbe
Main scribe: self
Additional scribes: Peter G.
# of attendees: ca. 12

Main issues discussed:
SPML did not have a lot of uptake, and SCIM has a fixed schema that is not supporting all use cases. What to do if an attribute set is already defined on the WebSSO channel, but one needs to do the same for upfront provisioning.
Use cases: group management, de-provisioning
Peter Gietz: implemented a solution based on SPML, Now often just using RA-part of the big SPML engine and do custom provisioning without SPML documents. SPML still Good for big environments, stable, functional. We had proposed a SPML to SCIM gateway, but did not found an implementation so far.
Evolveum has been developing enterprise provisioning solutions. This is a custom environment, customization is possible, standards are less important. SPML is missing the standard schema, there are no profiles. (DAASI is using DSML with LDAP schema standards). SCIM is better because it has a standard schema.
Atos has a product for health care market, using HL7 (provisioning in Health sector) with standardized schema for patient context. Could be reused in other spheres

The UK identity assurance program has the minimum data set.

“Lets revive SPML since it uses compatible schema”
DAASI has an extension to SPML to locate data if an identity changed in the target.
Another extension is to bulk upload it from scratch
But still SPML is complex.(just as SAML is) and SCIM might be to simple (just as OpenID Connect).
Messaging: SOAP or new standard wrapping SAML Attribute statements in a lightweight protocol.
Messaging is complex but needed
GRnet is running a central European messaging system. Client is initiator of the request and has possibility to cast and to retry.
How to provision clouds from multiple IdPs?.
GÉANT bus (Diego Lopez)
Greek solution is sort of based on these ideas.

Using messaging infrastructure. Some issues are between connecting clients to messaging server - needs local queuing. I a very widely distributed infrastructure it is difficult to synchronize interfaces - wrap it with library.

Insights / action items / next steps:
Complementary discussion in session 10/D “Long-term consistency & de-provisioning in SAML & OIDC”

18 Scalability, security, availability of services when you are not Google/Amazon

Convener: Pieter van der Meulen (SURFnet)

Main scribe: Markus Sabadello

# of attendees: 15

Main issues discussed:

Hard to build high availability, scalable, reliable systems.

1. In a few years everybody will use amazon-style cloud services?

Jurisdiction, privacy issues?

2. If there was a local, national "google data center", would you use it?

No guarantee where data will be stored?

E.g. in czech republic, must have private data in "cesnet" or at universities

3. If there was a Czech cloud service company "like" amazon/google, would you use it?

Probably not, would still want to keep data locally

4. Big problem: distributed, redundant databases

How to keep data consistent across different data centers?

Just “assume” that our data center will be fine?

Use VMWare virtual machines that can quickly replace each other.

5. UPS experience:

Two data centers 15-20km apart, still barely works with synchronous protocols. Not more.

6. Way forward?

Design our own Google-style data center?

Try to separate your application logic from data.

7. What are you trying to protect against?

Small failures, e.g. network lag, hard disk problems

Catastrophic failures, e.g. damage to data center

If you have multiple data centers, most failures actually come from the high-availability software itself.

Plan what is acceptable under what conditions (e.g. in the case of a big problem, session loss is OK, you just have to log in again)

8. Session management?

Use cookie-based load balancing, i.e. one user always interacts with the same server, “sticky” session is only kept there, not shared

9. Benchmarking

Run tests to actually find out what your scalability limitations are.

In SAML, the login itself is not very resource intensive.

In SURFnet, can do a few hundred logins per second.
10. Deployment
SURFnet using ansible now, want to move to Docker.
In Docker, keep code separate from data.
Don’t put SSH server in it.
Export the same ports for the same Docker container on every machine.
Don’t modify Docker images, just use them, don’t use ansible/scripts/etc. inside your Docker image (=anti-pattern)
How to distribute your Docker images? E.g. use CoreOS
11. Database synchronization between data centers
E.g. MySQL replication with read-only slaves
NoSQL databases, e.g. MongoDB?

19 letsencrypt.org for OV + EV certificates

(EV: extended validation, OV: organization validation)
Convener: Brook Schofield
Main scribe: Markus Sabadello
# of attendees: 13

Main issues discussed:

Mozilla, EFF, IdenTrust, etc. initiative info at http://letsencrypt.org/
For DOMAIN-validated certificates, probably with upsell model by IdenTrust https://www.identrustssl.com/
Deploy Python script on your webserver, solves hassles of getting low assurance certificate
Currently investigating within eduROAM/GÉANT to apply the same principles to a RADIUS/TLS (aka REDSEC) system.
Concerns that letsencrypt is only half of the steps, extra Apache configuration is needed for security, e.g. disable insecure ciphers
System admins might just run letsencrypt on the command line and think they're done (need to maintain your systems).
Experience: Lots of services have really bad certificate deployments (e.g. using SSLlabs to test)
Debian weak keys: Not updated in a long time - only because CAs check this - has the problem largely gone away.
If letsencrypt succeeds, is there a risk browser vendors may remove IdenTrust from their list of trusted CAs? No for Mozilla :-)
Why is OV/EV not used more? Problem is not price, but administrative burden
Admin problems with renewal (what exactly did we do three years ago to make it work?)
SHA-1 is getting deprecated, Chrome may already display warnings
In letsencrypt Github bug list, what are the main complaints?
https://groups.google.com/a/letsencrypt.org/forum/#!forum/client-dev & https://github.com/letsencrypt/lets-encrypt-preview
SPDY: Google's single stream HTTP protocol, didn't really take off, but may re-emerge as HTTP 2 http://en.wikipedia.org/wiki/HTTP/2
Real soon: Move to Elliptic Curve certificates

20 SAML/OIDC part II

Convener: Roland Hedberg
Main scribe: Rainer
# of attendees: 11

Main issues discussed:
Protocol steps:

1. discovery
2. client registration

Then it depends on the flow

3. Code flow:: authentication request, gets back access code
4. Code flow: Token request, gets back access token (plus refresh token, id-token)
5. Code flow: user info (send access token, get user info)

The access token could be a SAML assertion.
A problem is the userinfo schema, which is basically the Facebook set, no roles, affiliation, etc.
The subject has the pairwise identifier, the sector identifier and the public.
There is nothing like an attribute authority, but normal, aggregated (includes provenance, can be signed) or distributed (URL to the source).
Mapping problem: the OIDC has a limited user into endpoint, But you could define a SCIM endpoint.
Most implementations add information to the userinfo endpoint. But then there is no schema check. Is it necessary? People think that schema checking is useful.
Roland tried SAML/OICD gateway in both directions. One implementation is in InAcademia.

OIDC in mobile: work is going on in OID-foundation and GSM association.
In SAML IDP and SP are of similar complexity to implement. In OICD the RP is much simpler, whereas the OP is more complex.
The complexity of SAML comes also from XML processing.

21 “Something” as a Service for Identity Federations

Convener: Marina
Main scribe: Steve Olshansky
# of attendees: 10

Main issues discussed:
GEANT3+ task Federation as a Service (FaaS) - goal is to enable more federations in EU
43 partners in project, ~20 not having federations
Market analysis and conversations with NRENs identified issues:

- NREN-level
    - staffing issues
    - No SPs (chicken and egg problem, hoping eduGain will solve this)
- institution-level deployment issues with AAI and IdM
    - IT staffing issues

Prioritized helping NRENs by reducing staffing needs for federation operations.
FaaS offering
uses Jagger as Resource Registry
metadata aggregation and signing with HSM
close to being offered to NRENs
a lot of interest…
FaaS Market Analysis document http://issuu.com/danteprm/docs/ms83_ms5-4-1_federation-as-a-servic/1?e=6131560/7492653

DFN hosts IdP for its some of its institutions, but not their user DBs as campus uses their own IdM. Its free of charge service.
comment: There would be Interest in a pan-EU version of this, especially for smaller institutions. Q: Sustainability model for this?

Hub would be the ultimate FaaS scenario (e.g. SURFnet)

SURFnet looking at providing pre-configured options (config files and ARPs for Shib) for common services, to help some institutions to get past the complexity hurdle.

Finland provides attribute release policies as a service, with a web UI for custom tailoring of metadata for individual IdP/SP
Also outsourced IdPoLR, as does SURFnet through a commercial provider
Finland is thinking about Second factor authentication as a service.

Finland provides aggregated statistics aaS. The data gathered is number of logins for IdP, SP pair. Any person with Identity in HAKA can access the statistics.
comment: statistics is important for showing business value, help to identify which SP are or are NOT being used which can be interesting for licence recalculation.
Also useful for IdP admins

SURFnet will provide separate discovery service for eduGAIN SPs
ARP management seems to be very hard for many IdPs, so providing a service for this is very helpful
Need filtering for eduGAIN SPs since many are of no use to many SPs, and are just noise

Rainer’s tool Schematron enables schema validation, very useful.

GARR does similar to DFN IdPaaS, and also hosts userDB
Serbia has many institutions that have very limited existing infrastructure, so IdPaaS would be useful
K-12 schools are another community that would need hosted central services.
Added complexity is the need to register parents/guardians etc. as well, and this can be a big problem..

SURFnet offering protocol translation services. Piloting SAML-OIC, but not in production with this yet.

22 Delegated users management in customer facing services

Convener: Kari Nousiainen
Main scribe:
# of attendees:

Kari's presentation (slides as PDF)

23 Using non-academic identities in R+E federations (STORK, UnitedID, ..)

Convener: Enrinco Venuto
Main scribe: Rainer
# of attendees: 8

(see also notes from session 2 Auth Bridge between STORK and eduGAIN)

Main issues discussed:
Polito is outside the IT NREN federation. Need to work with people outside the academic sector - problem to enter the federation. Would have to filter the non-academic users.
In GRNET there is no limitation to academic-only users. There are e.g. hospitals.

The problem is hat eduGAIN is too light on that quality.

If WAYF would provide a STORK-like quality would that solve the Polito problem – Denmark will notify NemId in the coming years.

STORK does not support pairwise identifiers. Would have to be added in the gateway.
STORK can convey LoA - not only high assurance.

Some research communities need higher assurance. They do it through step-up authN, to avoid to have high assurance for everybody, but make it payable only the relevant users.

Insights / action items / next steps:
Participants agreed to coordinate their dislocated discussions. Steve and Rainer to propose a problem description. The existing STORK/SAML mailing list with REFEDs was considered as a common mailing list, however it might make sense to rename it.

24 OpenID Connect OSS development and Interop with SAML

Convener: Peter G.
Main scribe: Roland
Additional scribes: : Pieter, Peter
# of attendees: 14

Main issues discussed:
Given our (Higher Ed) experience with SAML and SAML federations there are things we need in OIDC that isn't there today.
How do we get them into OIDC and who will do it ?

What is missing in OIDC compared to SAML?

- Attribute set in OIDC userInfo is limited. It is basically the "Facebook set". No roles, entitlements, etc.
- Three party trust model: Federation Operator, RP, OP
- Transient NameID does not map to anything in OIDC

Scope of work to do

- Schema and attribute mapping
- Metadata handling
- Trust model (also in discovery)
- Proxies to SAML world (including OP and RP descriptors for SAML federations) ?

What libraries are available?
There are libs available: Python, 3xPHP, 6xJava, C#, C
There are "products" available: e.g. MS-ADFS, Azure AD, Ping,
All are doing OP rather than RPs.
Roland Hedberg is working on a test tool for OIDC implementations. I.e. test whether products and libraries are standard compliant.
Java library from MITRE put in Open Source and the one of Michael Schwartz (GLUE)

Python by Roland with GEANT funding, SimpleSAMLphp by SURFnet ?
Lets go bigger and try to have it in every library

We should try to get the Shib consortium involved to commit to OIDC implementation in Shib 3.X
Everything needs to be tested against Rolands test suite.

Insights / action items / next steps:

We do need to write enhancements down. Roland wants to start a document that in a later version could be inputted into the core OpenID group
This activity should be hosted within REFEDS (Roland talks to Nicole)
SURFnet/DAASI will contact the SimpleSAMLphp people.
Nicole will start a REFEDS subgroup with mailing list where we can discuss the spec.
At a particular point of time people like John Bradley, Hans Zandbelt, Mike Schwartz, SimpleSAMLphp etc.

25 Automated testing

Convener: Mads Freek
Main scribe: Rainer Hörbe
Additional scribes: Anders Lördal
# of attendees: 16
Main issues discussed:

Mads demonstrating the test environment from WAYF. The test tool does functional testing simulating a SAML IDP and SP. The test configuration is using a local configuration based on real configuration. The response message is parsed. Sometimes invalid messages are posted.
Mads is showing MARKUS, the operational statistics web page. (Is available as OSS on request). Authentication is simulated, not really tested.

SURFnet is using an external service to do a “chain testing”. Can do this from 46 nodes globally - gives an idea about the service quality. Used mainly for monitoring. SURFnet’s platform is made of many components, We do unit tests; use selenium for the web browser test, testing the negatives and key flows. Mock IDP/SP (“Virginia”) as part of this environment. Allows to set via REST the mock entity before creating the request.
Selenium: great if its works, but very version/configuration dependent. Have some 50-100 tests. Another method is to increase logging level of “Engine“ (the proxy piece) on production servers specifically for a pair of IDP/SP and analyze that log. There are instruments to adjust time slacks.
Production servers are clustered in sets; one is only accessible from the intranet. That one is using production data, but can be used for tests. In future new software will be deployed on one production node, will compare the behavior with previous version.
Using SAML tracer as well. SURFnet made an extension and pushed it to Feide. In the meantime it is available on the SURFnet wiki,

Rainer / Roland: saml2test cli tool (Github), web GUI available (STHREP on Github), tests both SPs and IDPs. Includes a suite of tests, sharing is encouraged. REFEDS will sponsor an instance.

Roland, Entity category tester, will test if an IDP will support specified entity categories and releases the correct set of attributes.

Count difference between Authn requests coming in and Responses going. When this metric changes (for a SP) this shows a potential problem.

Rainer presented SAML-Schematron (Github) in the last minute - extended metadata checks.

26 Enabling Change Within Federations

Convener: Ann West
Main scribe: Ann West
# of attendees: 6

Main issues discussed:

1. Enabling practice and policy changes such as attribute release which requires IT to engage policy people.
2. Enforcement - when do we do it, how and for what items

To effect legal/policy changes, SURFnet offers workshops for the law and privacy people to educate them on policies. SURFnet hires lawyers to weigh in on decision and verify it and communicates that to the community. SURFnet helps schools with privacy legislation as well. Their schools trust them to develop education and reports. They enforce practices that related to security on an ad hoc basis, that is they don't have a specific set but enforce as issues come up. To help with enforce, SURFnet hires students to call the operators and remind them of upcoming deadlines. However, because they have a small number of IdPs, the Surfnet knows the campuses and services providers. That personal trust contributes a lot.

Switch offers an automatic configuration option for ARPs. IdPs can always scope it or change it but most don't. Switch has a requirement to refresh the signing certificate every 3 years. They enforce this and the net effect is that it weeds out unsupported IdPs and SPs.

In RENATER, campuses each have a security officer who meet and decide what to do for their own campus. RENATER provides ARPs as well as static config files and provide the tools to change it.

Do we need to spoon-feed the ARP? If yes, then they have to trust us. The biggest issue with ARP is that the decision doesn't get made (who should make the decision on a campus? What's the process) so it's easier not to release them.

Do any have identity management requirements? Mostly no, but InCommon is starting to go there for specific things that contribute to trust and interoperability such as persistent identifiers.

Insights / action items / next steps:
Don't Worry be Happy.

27 To consent - or not to consent - info from the real world

Convener: Mads Freek Petersen
Main scribe: Pieter van der Meulen
Additional scribes: :
# of attendees: 4

Main issues discussed:
Repeat presentation from David's slides of a presentation he gave a Mountain View @IIW.
WAYF is a hub-and-spoke-federation. The WAYF SAML gateway uses a centrally hosted discovery service. Login flow:
SP -> Discovery service (@WAYF) -> IdP -> WAYF SAML Gateway -> SP
Consent is shown after authentication at the IdP:
Consent page contains:

- Service you are about to login to
- Description of attributes passed and their values

User has the following choices:

- I won't accept this -> Can use service
- Yes I accept -> Passed on to service
- Yes I accept and store preference -> Passed on to service and do not ask again for 3 years.

Other options:

- Documentation
- Management of consent. Here a user can see all consents previously given and also has to option to withdraw them
- No support for optional attributes. Same set of attributes for a SP for all users.
- When ARP (i.e. the attributes that a SP receives) changes this invalidates a previously given consent. For this purpose a hash of the attributes is stored along with the consent.

Statistics of consent from WAYF (the company):

- 66% of logins use previously stored consent
- 12% of logins are shown a consent screen of those
  - 9% agree, no not store consent (i.e. be asked next time)
  - 3% remember consent (i.e. not be asked again)

Nice graphs. Response times to consent screen are about 5 seconds on average. People how choose "remember" take a few seconds more time.

28 Long-term consistency & de-provisioning in SAML & OIDC

Convener: Radovan
Main scribe: Rainer
Additional scribes:
# of attendees: 13

Main issues discussed:
This use case:
How to pull users and attributes and get updates it? This is used for users for who have not logged in for long time.
This is for example required when user logged in last time in January and an email is sent in August.
Other related use cases:

- IDP pushes identities to RP
- RP pushes changed attributes to IDP

Polling is out of question for larger communities. It is not possible within the SAML and OIDC standards.
Ubisecure has implemented on the IDP a REST interface where a RP (like a CRM) can query, also using queries for many users.
Options are aggregating queries/updates with local filtering; messaging could decouple RP and IDP and make th API a bit simpler.
An issue is if the user needs to consent to the attribute release, Difficult it user is not there.
An alternative is to get the delta for the full user set in short intervals,.
There is a SAML Notify Protocol proposal that might be useful. But it seems it is not used much. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-notify-protocol/v1.0/csd01/sstc-saml2-notify-protocol-v1.0-csd01.html

To support all 3 use cases SPML could be used. Extending SAML (“SAML CRUD”) would be fairly little code compared to SPML.

29 Attributes: enhanced LoA, provenance, source, validations, valid until, …

Convener: Peter Gietz
Main scribe: Scott Koranda
# of attendees: 18

Main issues discussed:
A user might have been identified so that some attributes are "highly approved" such as name that has gone through a real vetting process, but others may be less assured like email, which is just assessed by some automated process, and still others that are self asserted.
Previous discussion talked about approaches to categorizing different levels of assurance.
LDAP has the notion of attribute options, ie. givenName; lang-jp:<something> then givenName; lang-en: John Smith, maybe use attribute option with ";loa-1", ";loa-2", and so on. That was idea from a previous session.
Also considered provenance, ie ";provenance-self-asserted"
";source=http://…"
";valid-from"
";valid-until"
Peter Schober added that this was all discussed previously in Belgrade?
Question: If the information were in the IdMs, how to put the information into a SAML assertion?
Decorate OID approach? No, would break existing functionality.
Don't want to define an entire new set of attributes so as to not offend those RPs that don't care.
Have only those RPs that care to query over back channel to get information, perhaps using a different set of attribute names (an augmented) set?
<ns:AttribueValue scope="example.org">member</ns:AttributeValue> but problem in practice has been hard to access the "scope=", but so then tried to flatten the string (but making more complex which offends existing RPs that don't care).
So maybe add <ns2:XXX self_asserted="true"> (call this "properties" approach)
Technically possible to extend SAML in this way, but point out that everything invented here is universally unsupported from the start (of course).
Maybe send both "normal" set of attributes and then "enhanced"? RPs that don't care about enhanced would just drop/ignore them. Downside is having to define the new enhanced attributes and write parsers and the like. One participant decided not to use this approach because it is "not a clean protocol message".

If standardized on a new namespace and got it adopted could use the properties approach.
What would be the set of properties? That is, the set of property names (the values are not constrained). Right now property names are:

- provenance
- source
- valid_from
- valid_to
- loa

In more detail:

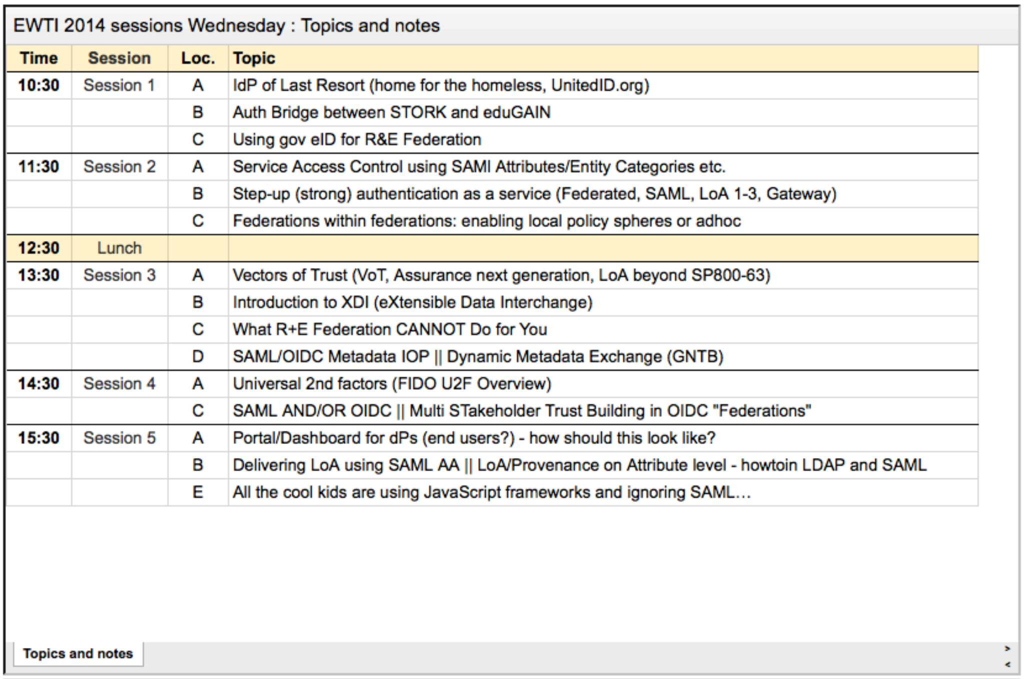
Name	Value (string, so free form)
loa	reference to practice statement
source	
source_type	
provenance	
verifier	
verify_method	
time_to_live	
valid_until	
valid_from	
original_issuer	
target_audience	

Question about how complex the ecosystem is with example of the post office selling address information versus self-asserted, so here the post office is a broker of attributes.
Bring up the point that some attributes are multi-valued, but with the "properties" approach the element is for attribute value, and hence each value has the opportunity to be "decorated" with these property names and the values.

Comment is that this is going the direction of building a taxonomy, and example from past is the authentication context taxonomy from SAML2. Debate on whether or not that was useful and bore fruit or was wasted effort.
Comment that some shared/controlled taxonomy or vocabulary can be constructed and useful, such as was this attribute self-asserted.

30 Session Time Tables

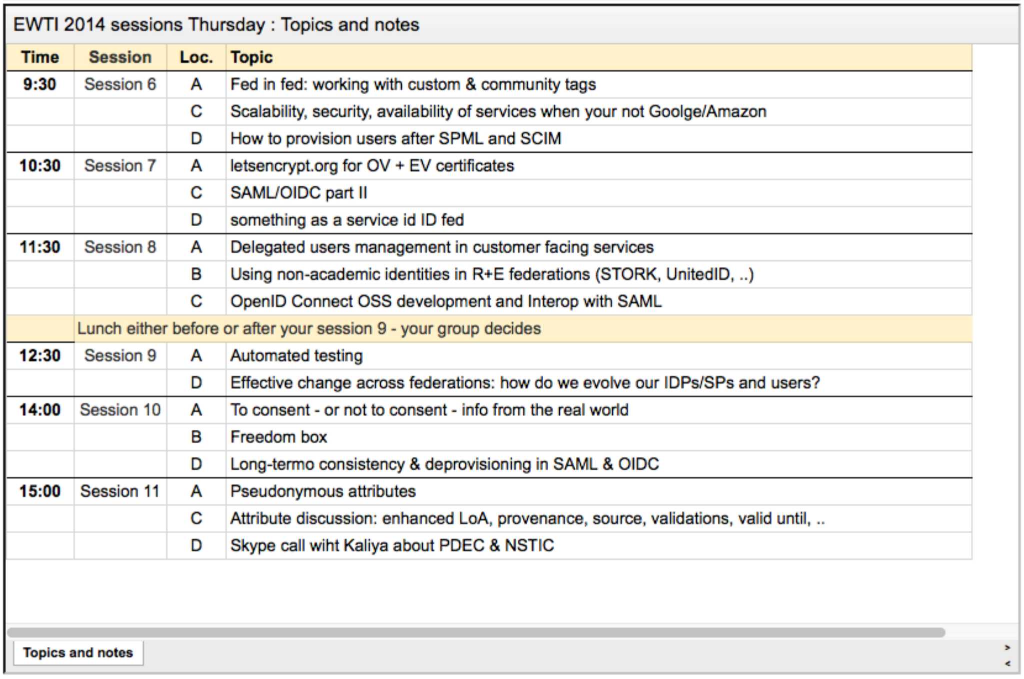
2014 sessions and notes



EWTI 2014 sessions Wednesday : Topics and notes

Time	Session	Loc.	Topic
10:30	Session 1	A	IdP of Last Resort (home for the homeless, UnitedID.org)
		B	Auth Bridge between STORK and eduGAIN
		C	Using gov eID for R&E Federation
11:30	Session 2	A	Service Access Control using SAMl Attributes/Entity Categories etc.
		B	Step-up (strong) authentication as a service (Federated, SAML, LoA 1-3, Gateway)
		C	Federations within federations: enabling local policy spheres or adhoc
12:30	Lunch		
13:30	Session 3	A	Vectors of Trust (VoT, Assurance next generation, LoA beyond SP800-63)
		B	Introduction to XDI (eXtensible Data Interchange)
		C	What R+E Federation CANNOT Do for You
		D	SAML/OIDC Metadata IOP || Dynamic Metadata Exchange (GNTB)
14:30	Session 4	A	Universal 2nd factors (FIDO U2F Overview)
		C	SAML AND/OR OIDC || Multi STakeholder Trust Building in OIDC "Federations"
15:30	Session 5	A	Portal/Dashboard for dPs (end users?) - how should this look like?
		B	Delivering LoA using SAML AA || LoA/Provenance on Attribute level - howtoin LDAP and SAML
		E	All the cool kids are using JavaScript frameworks and ignoring SAML…

Topics and notes



EWTI 2014 sessions Thursday : Topics and notes

Time	Session	Loc.	Topic
9:30	Session 6	A	Fed in fed: working with custom & community tags
		C	Scalability, security, availability of services when your not Goolge/Amazon
		D	How to provision users after SPML and SCIM
10:30	Session 7	A	letsencrypt.org for OV + EV certificates
		C	SAML/OIDC part II
		D	something as a service id ID fed
11:30	Session 8	A	Delegated users management in customer facing services
		B	Using non-academic identities in R+E federations (STORK, UnitedID, ..)
		C	OpenID Connect OSS development and Interop with SAML
	Lunch either before or after your session 9 - your group decides		
12:30	Session 9	A	Automated testing
		D	Effective change across federations: how do we evolve our IDPs/SPs and users?
14:00	Session 10	A	To consent - or not to consent - info from the real world
		B	Freedom box
		D	Long-termo consistency & deprovisioning in SAML & OIDC
15:00	Session 11	A	Pseudonymous attributes
		C	Attribute discussion: enhanced LoA, provenance, source, validations, valid until, ..
		D	Skype call wiht Kaliya about PDEC & NSTIC

Topics and notes