20190616 - REFEDS Annual Meeting topic proposals

Suggestions for the REFEDS 2019 agenda @TNC19.

Topic	Presenters	Time
FED2 Working Group Report	Tom Barton	
Assurance Working Group Report	Mikael Linden	
Sirtfi Working Group Report	Tom Barton	
Moonshot	Stefan Paetow	
FIM4R feedback	Dave Kelsey / Tom Barton	
Baseline: where do we go from here?	Workshop??	
# mRules ### Ian's rules for the rest of us WAYF has for many years used Ian Young's XSLT rules for checking metadata compliance. They are meant for use in a java environment and as we have used them from PHP we have not taken the full advantage of them. We have extracted the actual 'application logic' and combined it with a repository of xpaths and now we have a somewhat language independent wayf of expressing metadata requirements. We have implemented this simple logic in PHP, but it is our hope that others will implement it in other programming languages and contribute to the list of xpaths so we can get a common understanding of metadata requirements and an easily implemented way of actually checking them.	Mads	
# mEdit ### A schema-driven hierarchy-tabular metadata editor A core component in WAYF's new metadata repository system is mEdit, a schema driven hierarchy-tabular metadata editor with a bit of UX javascript added for extra usability. The editor is backed by a POGR (Plain Old Git Repository) which contains both the xml version and a 'flat' line oriented one for easy diff'ing and logging. The schema allows to do round-trip conversions between xml and some 'flat' formats for editing and logging.	Mads	
# SAML2jwt SAML2jwt is WAYF's new backend service that allows a service provider to connecet to WAYF (and thus to eduGAIN IdPs, using our 'eduGAIN-a-as-service' facility) in just 20 lines of code.	Mads	
# GUIdP In a federated world guest users, ie. users that does not have an affiliation to a home organisation is a special problem. They typically has to be provisioned for a service with yet another username/password. Some universities does run a guest IDP, but as there is typically not a central authority for doing identity proofing the level of assurance is often very low. For the services the guest login procedure needs be handled in a special way and for the guests it is yet another username /password to remember. The Grand Unified IdP solves this problem by separating the authentication from the identification: The guest once and for alle registers at an IdP that is able to recognise - ie. authenticate the user, but does not have any idea about the users actual identity. A service, that wants to allow a user access then creates a record in its user database with a username. This username is registered at the GUIdP in exchange for a token. The token is then communicated to the actual user in a wayf that satisfies the services requirements for identity proofing. The user registers the token in the GUIdP and links it to her login from the authentication IDP and is then able to login to the service. The service no longer needs to differentiate between ordinary federated users and guest users - login-wise. However the information that the GUIdP delivers is actually from the service's own userdatabase, the GUIdP acts as a service specific IdP. The GUIdP supports that services reciprocally can trust each other so a 'service' can be used as an IdP for other services - this is often labelled a virtual organisation. If a 'service''s requirements to identity proofing meets a federation's requirements it can be registered as a proper IdP in the federation - this is often called IdP as a service.	Mads	
# Attribute Value Filtering WAYF has started experimenting with expressing rules for attribute value filtering in metadata and implementing the filtering in our federation hub. The rules are just standard saml:AttributeValues for md:RequestedAttributes with an added @type with values: 'prefix', 'postfix', 'wildcard', 'regexp' that directs the actual processing.	Mads	
OpenAthens Discovery Service "WAYFfinder"	Jane Charlton	
AAF launched its Verification service (VerifID) in late 2018. They service is a lightweight API which allows commercial folk selling stuff to our community to verify if they are staff, student and get a Y/N response, ensuring privacy preservation. AAF has developed the technology, policy and business model (.35 AUD per verification) around the service and we now have three main customers using it. The good news here is that income from the service is helping to sustain the operations of AAF.	AAF / SheerID	15
NGI Trust	Brook	
GÉANT T&I ops.	Dick	
The future of federations in a Webauth world If IdPs don't get on board with releasing attributes, then SP/RPs will just interact directly with the user. What role do federations play in that scenario? • combo with Tom?? • SWOT approach??	Heather	