

EUGridPMA Day 1 - CESNET - Prague

Discussion of agenda - agreed.

Shows dates of upcoming meetings - see slide

Update from APGridPMA - see slides

Update from TAGPMA - see slides

Challenge of TAGPMA F2F meetings noted.

OIDC - Introduction - see slides from David Groep.

General intro plus description of IGTF OIDC Federation Task Force.

RPDNC is an important topic.

Snctfi is an important trust fabric to enable communities to easily join the federation.

Simplify by restricting to our RP and eInf use-cases.

Start by looking at some use cases, but all speakers are missing!

Start with Davide talking about AARC and GN\* recommendations.

There is already a standard for a dynamic registration (?)

See slides.

Trust is lacking. Discovery finds the OP but trust is missing.

There is a standard on OIDC Federation written by Roland on openid.net.

Key-signing being discussed - still need to check who is registering. Can have overlapping

communities - do not need to trust each other. "Community of Interest".

GN\* is considering either a hierarchical model or a parallel structure.

Others join

Michal P tells us about ELIXIR requirements/use cases.

There are no slides - just a short presentation. No big problem of registration of clients.

But new services are more likely to use OIDC, so having to do many new registrations will be

annoying. Would like to have a federation to register new clients and manage all the technical info required.

Discussion on why we have to trust SPs and RPs? DaveK was confused. Christos also confused especially in relation to scalability of building trust with a large number of SPs

Easier and more scalable to build trust between infrastructures using Snctfi rather than having to drill down into individual community and RP practices to look at differences between infrastructures.

Change management and revocation is difficult. What is key lifetime?

— coffee —

Jim B presents - and also represents XSEDE plans in absence of any XSEDE rep here at the meeting. XSEDE very interested in IGTF work on OIDC federation. Namespace ownership is important. Attribute Authority assurance profiles are important.

Scitokens.org is all about federated authorisation. Looking at OAuth Token Exchange.

scitokens - if you know issuer, metadata is always in well-known location.

client registration is a real important topic - just forgot to put it in the slides.

for CILogon they use R&S flag to avoid commercial clients. Interested in dynamic client registration in OPIDC Federation.

Scaling of RPs to be tackled hierarchically so just assess the Research Communities (of order 100 globally).

EGI Checkin and EUDAT B2ACCESS Use Cases - Nicolas.

see slides.

If we can solve the registration process, how do we then check/confirm that the client should stay in the registration.

Marcus talks about WaTTS - see slides.

A different use case from the dynamic registration of clients is the OIDC-Agent - slide 5.

Dynamic registration is crucial for success. JimB finds Marcus's OIDC-Gen very appealing.

We should aim to agree how to do this and maintain interoperability. Nicolas says the same for EGI.