

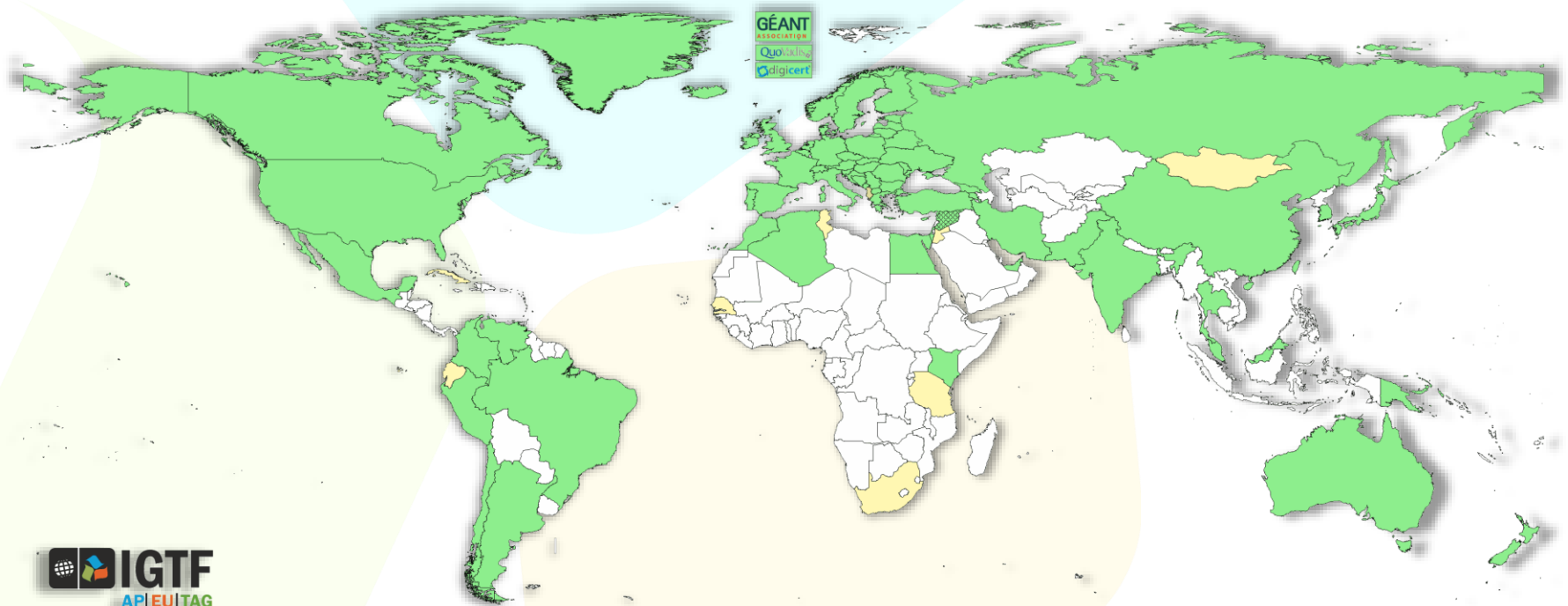
Leveraging the IGTF authentication fabric for research

*the IGTF-to-eduGAIN Bridge
and the registration authority
network*

David Groep
Nikhef



A look at the IGTF



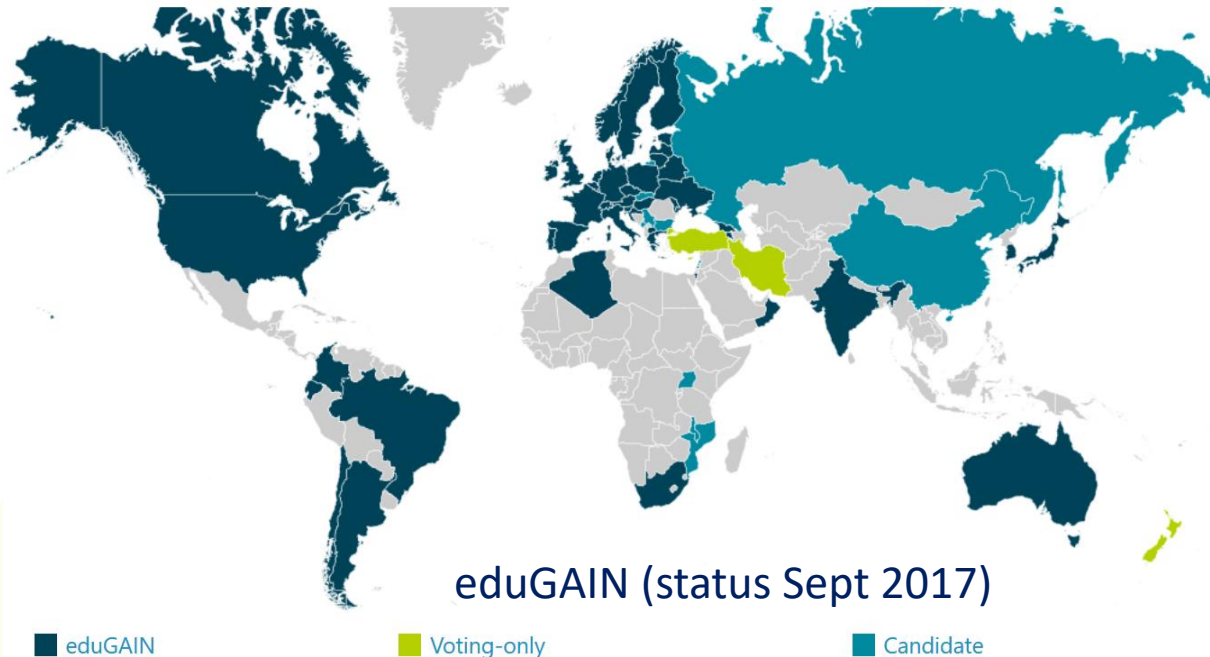
IGTF capabilities

- AuthN fabric and identity availability (today)
- Assurance requirements and assessment for Infrastructures (tomorrow morning)
- Registry operational guidelines (tomorrow morning)
- Infrastructure policy harmonisation *Snctfi* (tomorrow)
- Registry and operational capabilities (tomorrow afternoon)

What we do (for authN services)

- *User-centric* authentication – across organisations
 - Independent of user's home organization
 - Inspired by and aligned with research communities and e-Infrastructures
 - Differentiated assurance derived from a both solid and transparent assurance level
 - Ability to transfer registrations across authorities and countries (with the Registration Practice Statement)
- ... and guidance around trust and trustworthy operations for AuthN and Attributes ... and ...*

eduGAIN



- 40 NRENS (\approx countries)
- 4254 entities
(of which 2533 IdPs, *i.e.*, authentication providers)

- organisation-centric, and with much national autonomy in policy & practice
- where it reaches the users *and* a 'link' is made, provides great ease of use
- in most organisations, research is not the primary use case (yet) for the 'IdP'

Infrastructure specific hubs

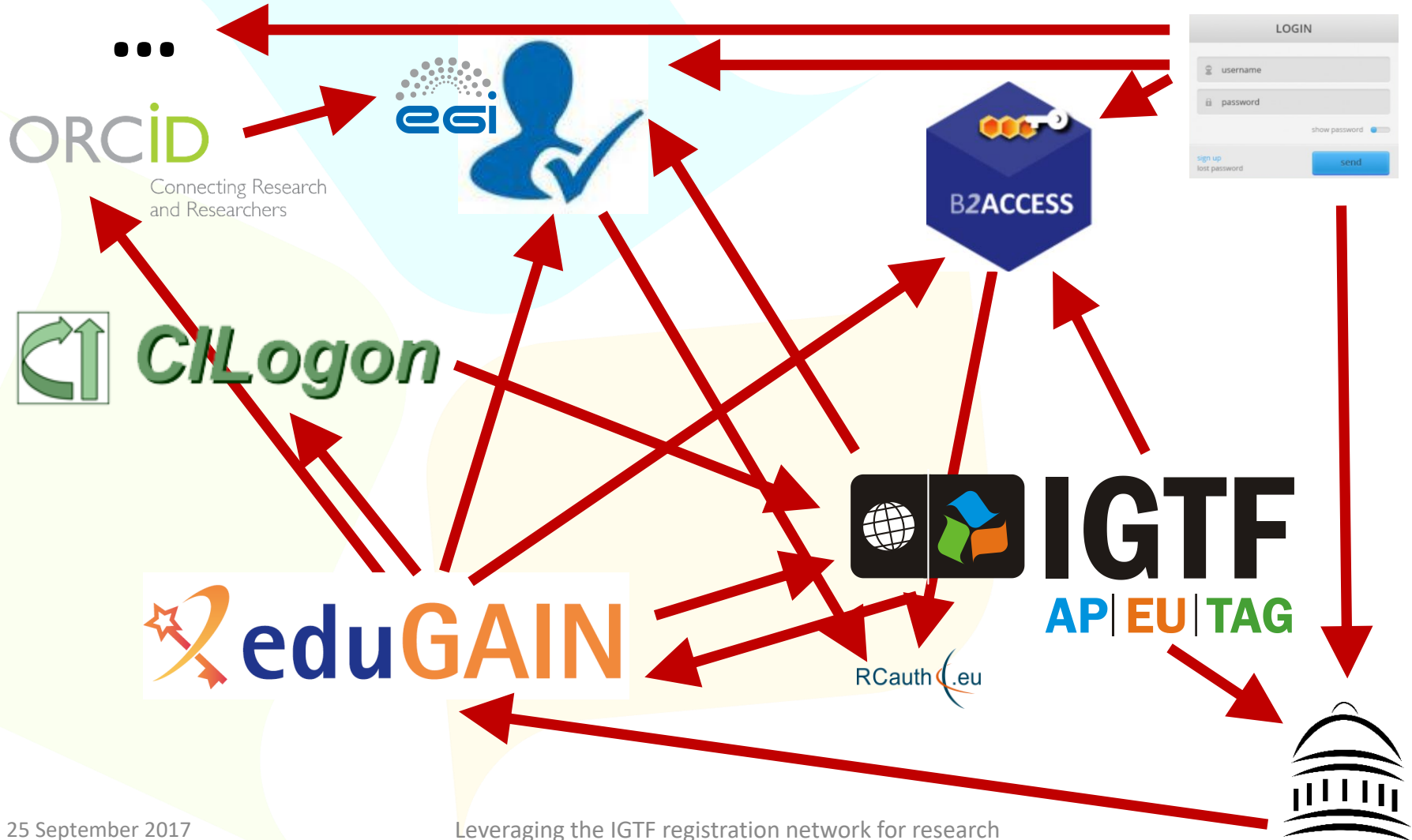
- EGI CheckIn
- B2ACCESS
- CILogon
- ORCID
- ...



Service-bespoke solutions

- ~~Local log-in, mangled tokens, directory auth, 'golden' portals that don't keep your credentials, 'golden' portals assuming ownership of everything, ...~~

Turtles all the way down ... and up!



TCS – CILogon – DFN SLCS – RCauth.eu

RCauth.eu The white-label Research and Collaboration Authentication CA Service for Europe

RCauth.eu Online CA consent page

The Master Portal below is requesting access to your personal information and...
If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and how they are processed...
For further information on the CA see the RCauth.eu homepage.

Remember

Master Portal Information:

Name: EGI Master Portal
Description: EGI Master Portal
URL: https://masterportal-pilot.aa1.egi.eu

Information that will be sent to the Master Portal:

sub : davidg@nikhef.nl
idp : https://sso.nikhef.nl/sso/saml2/idp/metadata.php
eduPersonTargetedID : https://sso.nikhef.nl/sso/saml2/idp/metadata.php
idp_display_name : Nikhef
cert_subject_dn : CN=David Groep QK-DHKZMTHoVTT6,O=nikhef.nl
name : David Groep

DigiCert® | CERTCENTRAL®

IDP Selection

Please enter the Identifier

Nikhef

CILogon

Select An Identity Provider:

- IFSULDEMINAS - Instituto Federal de Educac
- IFTM - Instituto Federal de Educac
- IFTO - Instituto Federal de Educac
- IGTF**

Search:

Remember this selection:

By selecting "Log On", you agree to [CILogon's privacy policy](#).

DFN-AAI Deutsches Forschungsnetz

[About DFN-AAI](#) | [Help](#)

Select your organisation

In order to access the service **DFN Short-Lived Credential Service (DFN-SLCS)** please select or search the organisation you are affiliated with.

Enter the name of the organisation you are affiliated with...

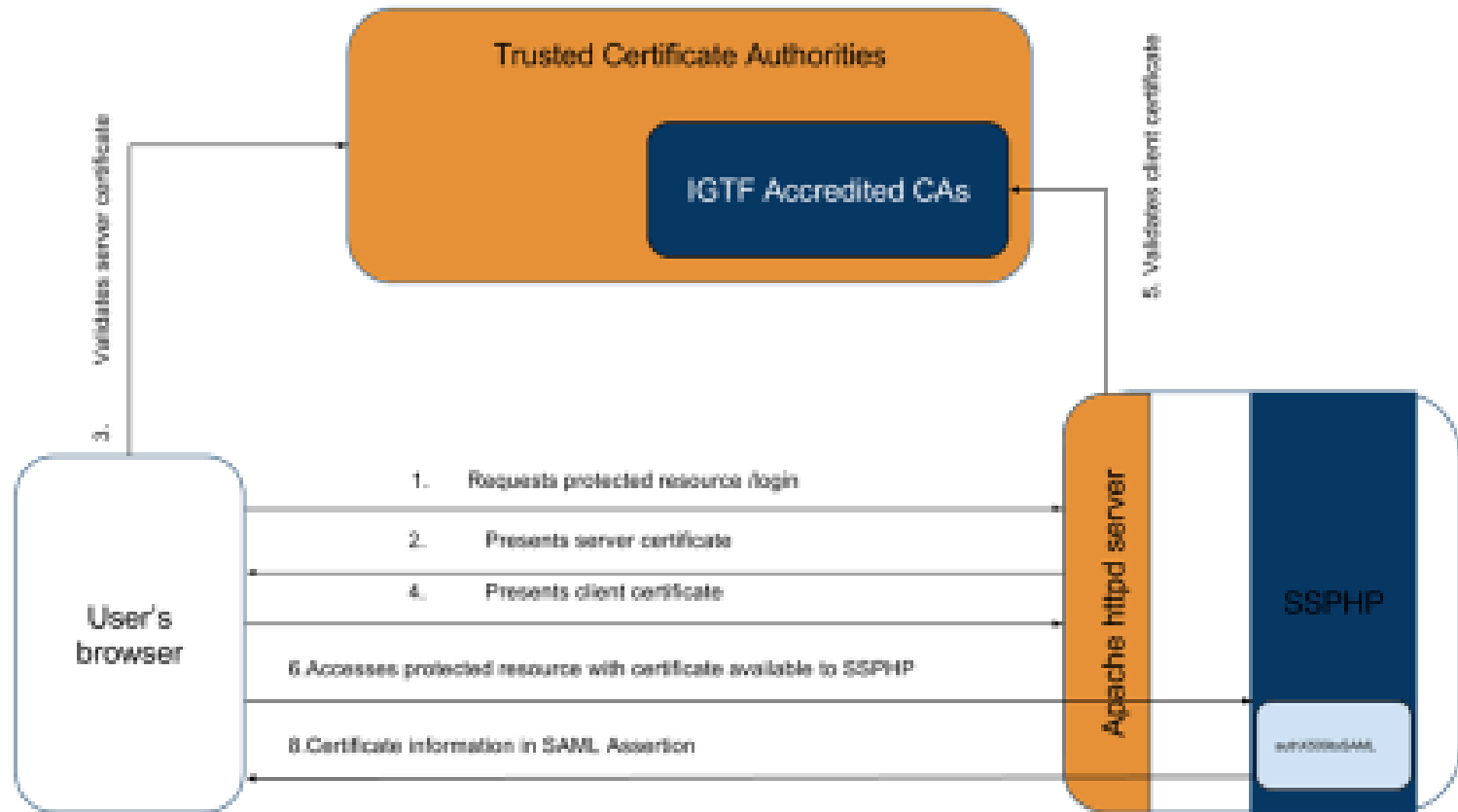
- Academy of Fine Arts Leipzig
- Albert-Ludwigs-Universität Freiburg
- Albstadt-Sigmaringen University of Applied Sciences
- Alfred-Wegener-Institut für Polar- und Meeresforschung IdP
- BA Glauchau
- Bedische Landesbibliothek

ed by SWITCH

Leveraging the IGTF registration network for research

Bridging IGTF to eduGAIN

authX509toSAML



Guidance we have and use

Assurance Profile

- <https://www.igtfn.net/ap/>

Assessment support

- <http://wiki.eugridpma.org/Main/AssuranceAssessment>

'Back-office' template practices

- <https://www.eugridpma.org/documentation/rps/>

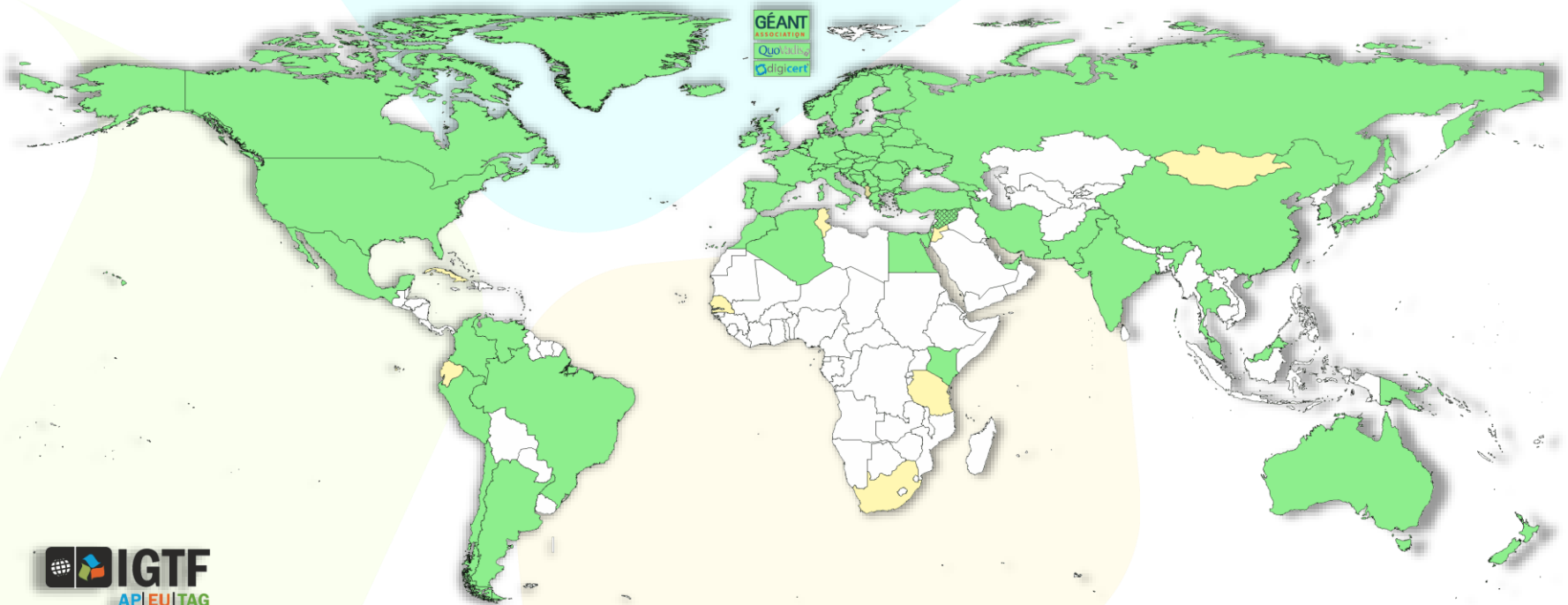
Registration Networks

Although the process is labour-intensive and relatively slow, for some user categories the prevalent 'user-held' credential is the only one that 'works':

- non-academic users (SMEs, industrial R&S)
- users in a place without an eduGAIN federation
- users in a place that does not do unique ID
- users in an organization that does not release attributes
- users in an organization that does not provide assurance
- ...

A 'high-quality IdP of last resort'?

- Most useful asset is our RA network!



Ideas ...

- Promote the use of (existing) bridges
- Support other credential types and/or interfaces?
- In places without an existing federation
 - Promote its establishment, as now eduGAIN is more open than before ...
 - join eduGAIN yourself – as a ‘trivial hub&spoke’ using the bridge IdP technology?
- Where a federation exists
 - Establish direct links – there’s an opportunity in ‘long-tail’ support and IdP-of-last-resort services 😊?
 - Push for a federation policy aligned with global (researcher) needs?
- Expose differentiated assurance model to subscribers?
- User-held credentials avoid much of the privacy issues?



Discussion!

BUILDING A GLOBAL TRUST FABRIC