# InCommon Assurance Call

# **Developments in Assurance: Insights from Across the Pond**

Wednesday February 3, 2016

Speakers:

- Daniela Pöhn, Leibniz Supercomputing Centre
- Mikael Linden, CSC - Finnish IT Center for Science
- Chris Spadanuda, University of Wisconsin - Milwaukee, Chair of InCommon Assurance Advisory Committee

# Assurance Advisory Committee

InCommon has been approved by the US government Identity, Credential, and Access Management program as a Trust Framework Provider at Levels of Assurance 1 and 2. This means that organizations certified at Bronze and Silver by InCommon are approved to interoperate with Federal agency applications requiring LoA 1 (Bronze) or LoA 2 (Silver).



5 Bronze, 1 Silver

- Bronze
  - Virginia Polytechnic Institute and State University
  - University of Maryland Baltimore County
  - Harvard University
  - University of Nebraska Medical Center
  - The George Washington University
- Silver
  - Virginia Polytechnic Institute and State University

# Participant Operating Practices (POP)

- Community Standard and Expectation
- Self developed
- Not machine readable
- Some do not have
- Some have not updated
- Difficult to verify

# Assurance Advisory Committee proposal

- Five minimum requirements for IDP's
- Five minimum requirements for SP's
- Minimums communicated in a machine readable format.
- Creation of a business and technical processes to hold IDP's and SP's accountable for the five minimum standards

Further discussion this spring. A strawman!

# Division of responsibility between GÉANT and AARC in Assurance

GÉANT (GN4 project):

- Pan-European data network for research and education connecting the national networks (NRENs)
- Also EC-funded project developing the network and related services such as eduGAIN
- Level of Assurance one aspect
  - representing IdP-side realities

AARC project:

- EC-funded project to develop an AAI that fits researchers' needs (based on eduGAIN)
- Research infrastructure/community (=SP) driven
- Level of Assurance one aspect
  - representing SP requirements


Authentication and Authorisation for Research and Collaboration

# Minimal Level of Assurance (LoA)

## Recommendation for low-risk research use cases

**Mikael Linden**
AARC NA3.1 task “Level of Assurance”, task leader

InCommon Assurance call
3 Feb 2016

# Level of assurance
## Research community interviews done

- Interviewed 6 research infrastructures
  - CLARIN (language research)
  - DARIAH (arts and humanities)
  - ELIXIR (life science)
  - LIGO (physics)
  - photon/neutron facilities (physics)
  - WLCG (physics)
- Interviewed 2 e-infrastructures (cyberinfrastructures)
  - EGI
  - PRACE
- Interview results: https://wiki.geant.org/x/nQHbAg

# Minimum LoA recommendation (30 Nov 2015)

1. The accounts in the Home Organisations must each belong to a known individual
2. Persistent user identifiers (i.e., no reassign of user identifiers)
3. Documented identity vetting procedures (not necessarily face-to-face)
4. Password authentication (with some good practices)
5. Departing user's eduPersonAffiliation must change promptly
6. Self-assessment (supported with specific guidelines)

The document: https://wiki.geant.org/x/wIEVAw

# Community consultation 11/2015-1/2016

- Received 25 comments (mostly from federation operators)
  - https://wiki.geant.org/download/attachments/47907229/MinimalLoArecommendation--comments.pdf
- ”Is this a report feeding the actual profile work that will start”
- ”Need to involve more research communities to make them committed”
- ”This is an approximation of InCommon Silver which hasn’t gotten traction. Why would this?”
- Many comments expected more detail (that are specific enough to be auditable)
  - Unique identifier (”Don’t rule out ePPN”)
  - Password requirements
  - eduPersonAffiliation and departing users
- Mappings to existing federations policies

# Spin-off: Self-assessment tool

- Self-assessment proposed as the approach for ”IdP audit”
- A web based tool to support the IdP admins in the self-assessment
  - Presents the specific requirements as a check-list
  - The IdP admin goes through the list one-by-one
  - The tool evaluates the answers
  - If ”pass”, federation operator adds an Entity Category tag
- Software Requirements specification
  - Together with Sirtfi
  - https://docs.google.com/document/d/10kguCdxWn38z_EGRnrdjCI4GSeO44zFGeXWHGmzz27o/edit

# Thank you

# Any Questions?

Mikael.linden@csc.fi


https://aarc-project.eu


The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).

# Service Aspects of Assurance

## IdPs and Federations

**Daniela Pöhn**

SA5T1 Subitem Service Aspects of Assurance

Research Assistant Leibniz Supercomputing Centre

InCommon IAM Online

2016-02-03

# Survey on federations

https://wiki.geant.org/display/gn41sa5/Federation+survey

Results:

- LoA in place with contracts
- Identity Management Practice Statement, but not enforced
- Documented, but not enforced
- Most federations/IdPs do not want a higher LoA
- Impacts on adopting LoA: between none till high costs
- Hub-and-spoke federations have more control

# Survey on identity provider

https://wiki.geant.org/display/gn41sa5/IdP+survey

Results:

- Individual accounts
- Most IdPs have an identity vetting process, but not documented
- Most IdPs have certain password qualities
- (Almost) no second-factor authentication
- Update of account/affiliation between less than 2 weeks and more than 6 months
- Partly documented
- Partly Incident Response Process

# Baseline requirements and costs

- Individual accounts
  - without much manpower or high costs
- Persistent, non re-assigned identifiers
  - not re-assigned might take time
- Documented identity vetting, which is not necessarily face to face
- Password authN with some good practices
- Departing user's ePA changes promptly
  - might be more expensive or take manpower
- Self-assessment of LoA supported with specific guidelines
  - in contrast to audit

# Potential solutions

- Self-assessment template / tool:
  - GÉANT web tool
  - including recommendations and best practices
  - (combined with SIRTFI and other monitoring/testing tools),
- For IdPs, who need a higher LoA:
  - Peer (pairwise) auditing of IdPs
  - Second-factor authentication: GÉANT could offer it as a service or procure Duo-type solution for community

# Thank you

## Do you have any questions?

daniela.poehn@lrz.de

GÉANT

Networks · Services · People

www.geant.org

This work is part of a project that has applied for funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

## Final remarks/questions

Research is global

- a LoA framework is useful only if it is global

How to proceed to developing a global minimal assurance profile?

- Fulfills research communities' needs globally
- Is recognised by IdPs (and driven by federations) globally?

Thank you for joining the InCommon Assurance Call.

To join the InCommon Assurance email list

- email **sympa@incommon.org**
- with this subject: **subscribe assurance**