InCommon Assurance Advisory Committee

Monthly Webinar

January 4, 2017

REFEDS Assurance working group and profile

Mikael Linden, REFEDS assurance wg chair
mikael.linden@csc.fi

InCommon Community Assurance call Wednesday, Jan 4, 2017

Outline

- AARC project and researchers' needs
- REFEDS assurance working group
- Design criteria
- REFEDS Assurance profile (DRAFT)
  - Dimensions
  - Conformance criteria
  - Assurance levels
  - Representation on SAML 2.0
- Assessing the assurance levels
- Roadmap

AARC project – improving federations to serve the researchers even better

- AARC – Authentication and Authorisation for Research&Collaboration
  - European Commission funded project, 5/2015-4/2017
  - Coordinated by GEANT
  - 20 partners (from Europe), representing research infrastructures and federation operators
  - https://aarc-project.eu/
- A work item: Level of Assurance (LoA)
  - Minimal LoA recommendation for low-risk research use cases, 11/2015
  - Differentiated LoA recommendations applicable to research use cases, 3/2017

AARC deliverable 11/2015: a Minimal LoA recommendation for low-risk research

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

REFEDS assurance working group

- In 6/2016 REFEDS established the Assurance working group
  - Open to anyone to participate
  - Take AARC recommendation as input and expand it into a specification
  - International – participants from Europe&US
  - Cross-community – participants from federations & research communities
  - Bi-weekly calls and a specification on Google docs
- Now
  - The first complete draft on REFEDS Assurance profile nearly there
    - comments welcome: http://tinyurl.com/h8z3joe
  - Formal community consultation planned in early 2017

Design criteria for the REFEDS Assurance profile

- **Multidimensional** in opposite to monolitic
  - Assurance split to 4 dimensions
  - For simplicity to SPs, dimensions also collapsed to scalar levels
- Stick to **simplicity**
  - Don’t overdo it or it won’t be used
- **Don’t re-invent** wheels
  - Instead, refer to existing work like Kantara SAC and eIDAS assurance levels
- Cover the needs of **international research** collaborations

Dimension 1/4: Identity uniqueness

`$PREFIX$/ID/unique`	• User account belongs to a **single** natural person • The person is **traceable** • The user identifier is **not re-assigned** • The user identifier is one of these: eduPersonUniqueID, SAML2 persistent ID or eduPersonTargetedID

Extra values describing eduPersonPrincipalName (ePPN) re-assignment practice:

`$PREFIX$/ID/ no-eppn-reassign`	ePPN values are not re-assigned.
`$PREFIX$/ID/ eppn-reassign-1y`	ePPN values may be re-assigned after a hiatus period of 1 year or longer

Dimension 2/4: Identity proofing & credential issuance, renewal and replacement

`$PREFIX$/IAP/local-enterprise`	The identity proofing and credential issuance, renewal and replacement are done in a way that qualifies the user to access the Home Organisation's **internal administrative systems** (e.g. finance or student information system).
`$PREFIX$/IAP/assumed`	Identity proofing and credential issuance, renewal, and replacement qualify to any of • Kantara assurance level 2 • IGTF BIRCH (which refers to Kantara AL2) • eIDAS assurance level low
`$PREFIX$/IAP/verified`	Identity proofing and credential issuance, renewal, and replacement qualify to any of • Kantara assurance level 3 • eIDAS assurance level substantial

Dimension 3/4: Authentication

`$PREFIX$/AAP/local-enterprise`	The authentication is done in a way that qualifies the user to access the Home Organisation's **internal administrative systems** (e.g. finance or student information system.)
`$PREFIX$/AAP/single-factor`	Authentication qualifies to Kantara assurance level 2. If passwords are used, their entropy must meet the requirements set by *AL2_CM_CRN#040,* unless REFEDS has agreed on a higher requirement.
`$PREFIX$/AAP/multi-factor`	Authentication qualifies to any of • Kantara assurance level 3 • eIDAS assurance level substantial • [a placeholder for the REFEDS MFA Profile once it is agreed on]

REFEDS MFA Profile to be exposed to a public consultation soon…

Dimension 4/4: Attribute quality and freshness

`$PREFIX$/ATP/ePA-1m`	eduPersonAffiliation (and derivatives) values “faculty”, “student” and “member” **reflect users’ departure** within the 1 months time.

Conformance criteria

To be able to assert conformance to the REFEDS Assurance profile, the Baseline Expectations of Identity Providers must be met:

1. The IdP is operated with organizational-level authority
2. The IdP is trusted enough to be used to access the organization’s own systems
3. Generally-accepted security practices are applied to the IdP
4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL

Collapsing the 4 dimensions into Assurance levels (for SPs who want simplicity)

Value	~~Minimal~~ Banana	~~Higher~~ Mango
`$PREFIX$/ID/unique`	X	X
`$PREFIX$/ID/no-eppn-reassign`		
`$PREFIX$/ID/eppn-reassign-1y`		
`$PREFIX$/IAP/local-enterprise`	X	X
`$PREFIX$/IAP/assumed`	X	X
`$PREFIX$/IAP/verified`		X
`$PREFIX$/AAP/local-enterprise`	X	X
`$PREFIX$/AAP/single-factor`	X	X
`$PREFIX$/AAP/multi-factor`		X
`$PREFIX$/ATP/ePA-1m`	X	X

Minimum LoA recommendation as defined in the AARC document

Representing the assurance profile on SAML 2.0

Value	eduPersonAssurance	Metadata entity attribute
$PREFIX$		X
$PREFIX$/ID/unique	X	
$PREFIX$/ID/no-eppn-reassign	X	
$PREFIX$/ID/eppn-reassign-1yr	X	
$PREFIX$/IAP/local-enterprise	X	
$PREFIX$/IAP/assumed	X	
$PREFIX$/IAP/verified	X	
$PREFIX$/AAP/local-enterprise	X	
$PREFIX$/AAP/single-factor	X	
$PREFIX$/AAP/multi-factor	X	
$PREFIX$/ATP/ePA-1m	X	
$PREFIX$/ATP/authoritative	X	
$PREFIX/LOA/minimal	X	X
$PREFIX/LOA/higher	X	X

Assessing the assurance level of an IdP?

- Currently not defined in the Assurance profile document

- Some initial discussion:

1. Self-assesment for items required for the ~~mimimal~~ banana level?
2. Peer-assessment for items required for the ~~higher~~ mango level?

Possibly assisted by a self-assessment tool

1. C.f. The AARC/GN4-2 Self-assessment tool: https://wiki.geant.org/display/AARC/Self-assessment+tool

Roadmap

- Expose the Assurance profile (DRAFT) to a community consultation
  - Starting in a few weeks?
  - Until end of March?
- Publish the version 1.0 in April?
- Have a pilot?
- Roll out

Questions?