Authentication and Authorisation for Research and Collaboration

Attribute Authority (and proxy) Operations

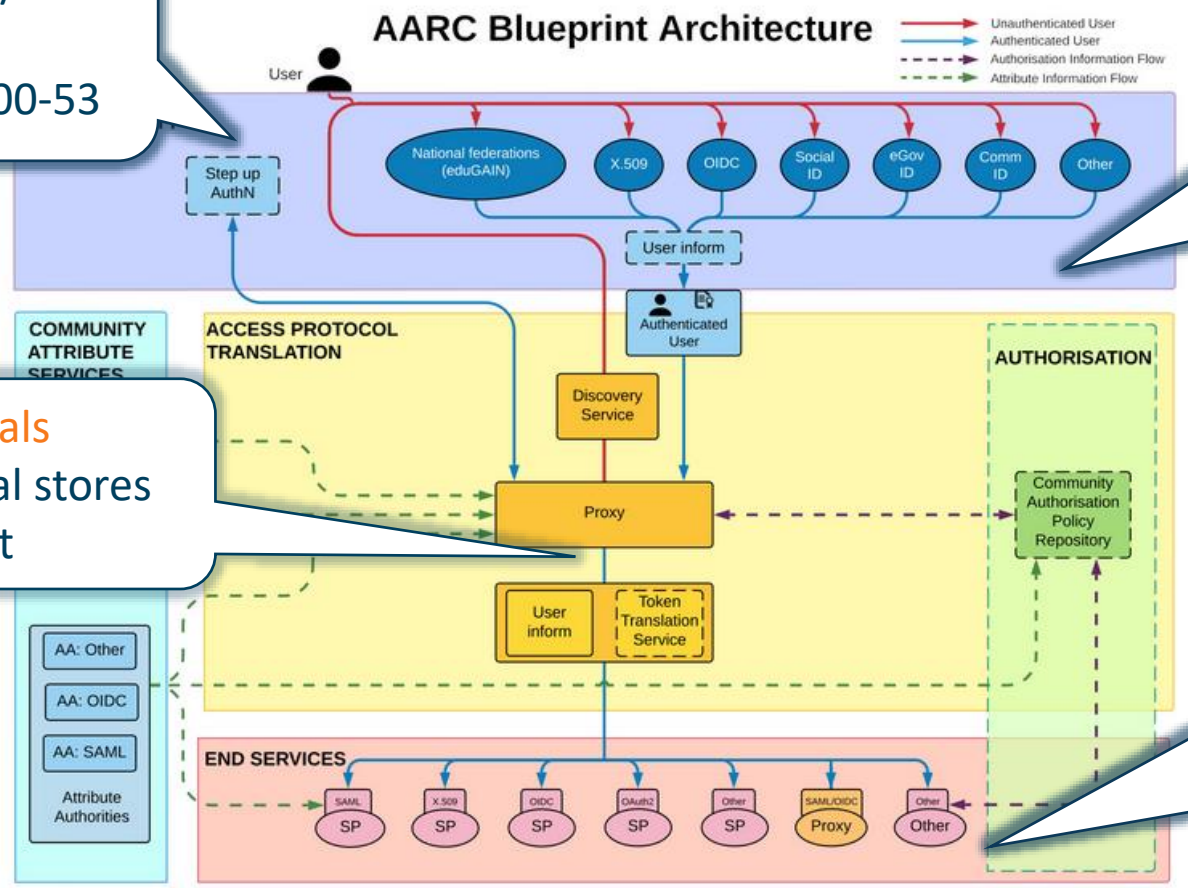
Completing the AARC G048bis process with ‘G071’

David Groep Nikhef
AARC Community Policy WG

AEGIS February 2022 meeting
2022-02-14

Operational guideline landscape for - proxy or source - AAI components

RFC6238/4226
FIPS140
NISTSP800-53



Authentication/identity sources
Sirtfi
(eduGAIN) baselining, RAF
IGTF AP Profiles
NIST SP800-63
eduGAIN sec. team workflow

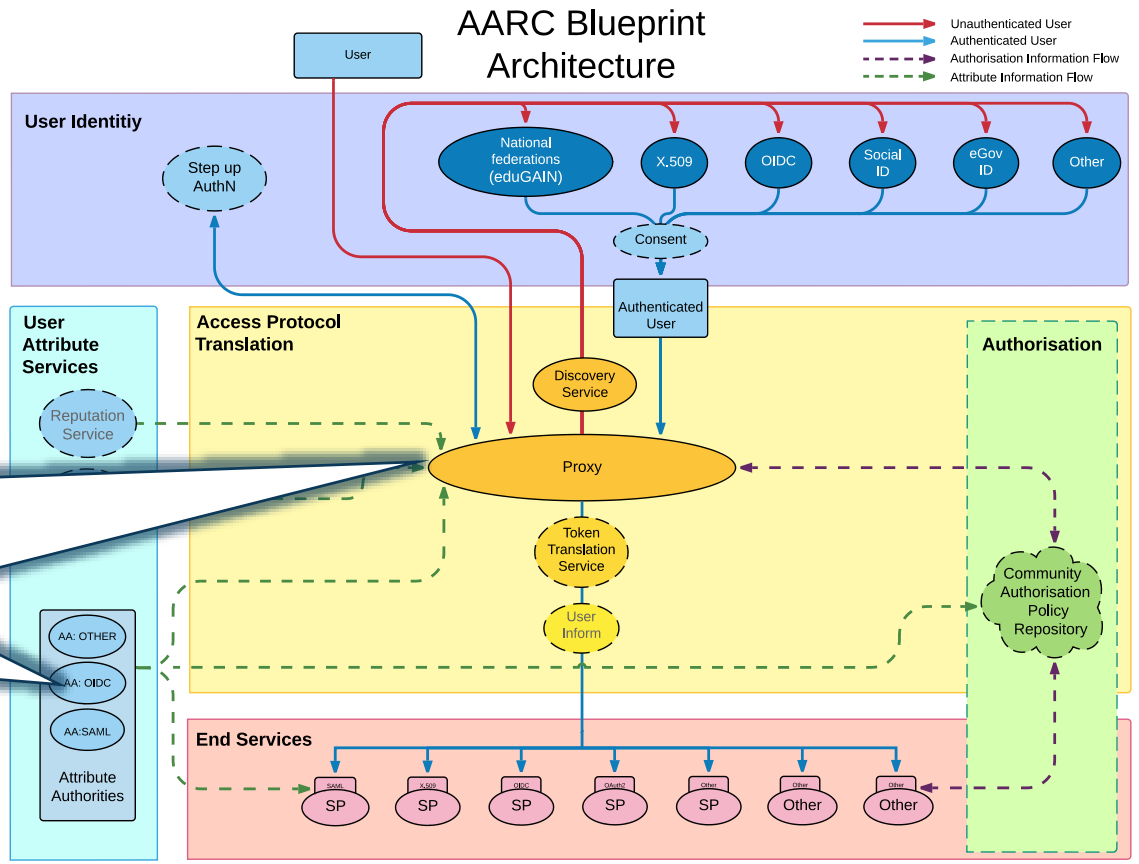
Ephemeral credentials
- trusted credential stores
- protection at rest

Service provider operations
ISO27k
Sirtfi
Infrastructure response plans

Operational security focus in the BPA: beyond just the IdPs

Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity

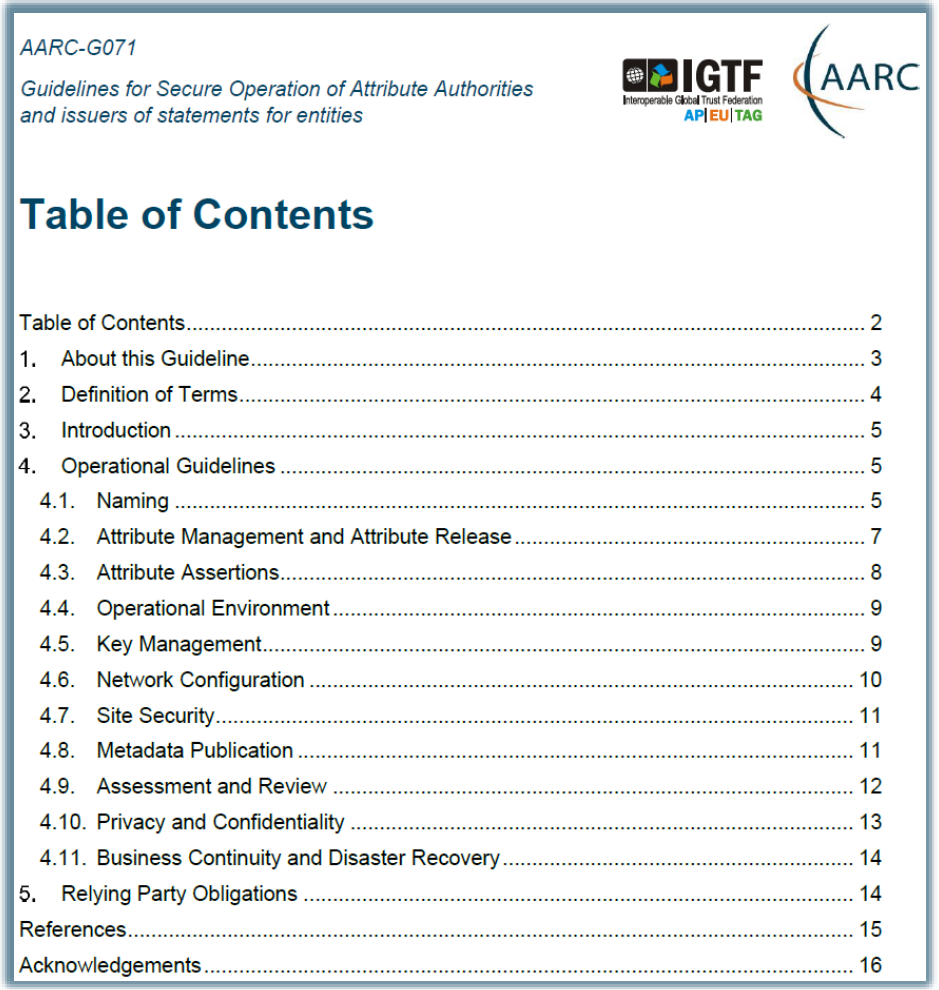


Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements
(AARC-I048, in collaboration with IGTF AAOPS)

AARC-G071: keeping users & communities protected, moving across models

Structured around concept of "**AA Operators**",
operating "**Attribute Authorities**"
(technological entities or proxies),
on behalf of, one or more, **Communities**, that are
trusted by **Relying Parties**

formerly AARC-G048bis



AARC-G071

Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

IGTF Interoperable Global Trust Federation AP|EU|TAG

AARC

Table of Contents

Deployment guidance included …

4.2. Attribute Management and Attribute Release

AMR-1

The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.

The community should follow the guidance from relevant policy documents. In particular, the Policy Development Kit has recommendations on Community Membership Management. It is recommended to use standardised attributes where possible, e.g. from eduPerson [EPSC] or SCHAC [SCHAC], and their semantics must be respected.

If Communities make modifications to the attribute set, their semantics, or release policies, it is recommended that they inform both their relying parties as well as the AA Operator thereof, since the AA operator may have implemented checks for schema consistency. The Community is ultimately responsible for the values and semantics of the attributes.

AMR-2

The AA Operator must implement the community definitions as defined and documented, for all the AAs it operates.

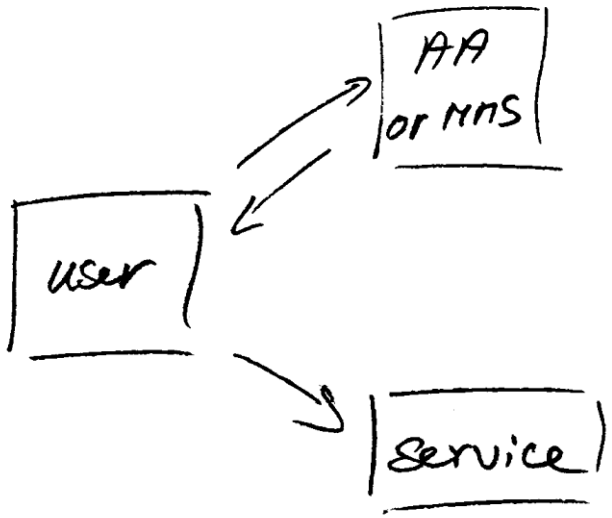
By implementing these requirements, the AA operator will support the chain of trust between Community and the RPs. An AA Operator must only host those communities for which it can implement the requirements.

AMR-3

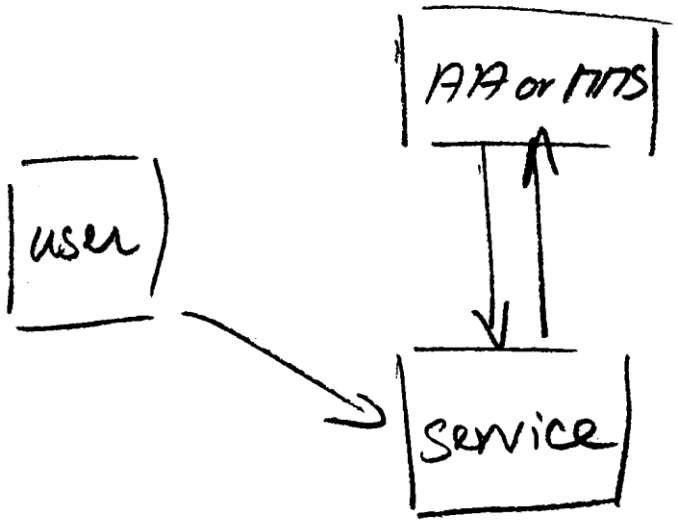
It is recommended that the AA Operator provide a capability for the community to

Protecting the community membership data and its proxy

Intentionally targeted broader than just the push model, since operational security spans data centres and infrastructures using other forms of AA membership management (SAML, OIDC, LDAP, …)



push model – the common BPA method (e.g. SAML AttributeStatement, VOMS AC)



pull model – common when using directories (e.g. LDAP in PRACE, userinfo endpoint in OIDC)

push and pull model diagrams as per RFC2904 – the 3rd (agent) model is uncommon in research/collaboration scenarios except for provisioning

When the AA is in a managed environment …

Many of the recommendations are already implemented 'implicitly'

- because common software implements it: e.g. signing SAML assertions and JWTs
- because a good data centre already has network monitoring and central logging in place
- because you signed up to Sirtfi (didn't you?) – so you collaborate in incident response
- because you have trained IT operations personnel looking after the service

And some are intuitive best practice

- like assigning a unique and lasting name to a group
- because implemented controls ought to be those that have been documented

Some items contain reminders about appropriate values and recommendations that are good practice - based on the relevant standards involved

Implementation of the AA Operations ("AAI proxy") Security guidelines

1. AEGIS, major RPs, and Infrastructures reviewed it in light of their the current (up-to-date) use cases and models
2. Guideline aims at both Infrastructure and Community use cases, in any combination – independent of their business relationships
3. Useful input to the EOSC connected proxies as a good practice guideline
4. Does not address any assessment or review process, but does state what needs to be logged and saved to make (self) assessment, and incident response, possible

https://aarc-community.org/guidelines/aarc-g071/

it incorporated much of your input as well – thanks for that! Now is your 2nd chance …

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-community.org

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme and other sources.