



Authentication and Authorisation for Research and Collaboration

Attribute Authority Operations Revisited

Completing the AARC G048bis process

David Groep

AARC Community Policy WG



EUGridPMA 54 meeting

2022-01-26

Operational guideline landscape for - proxy or source - AAI components

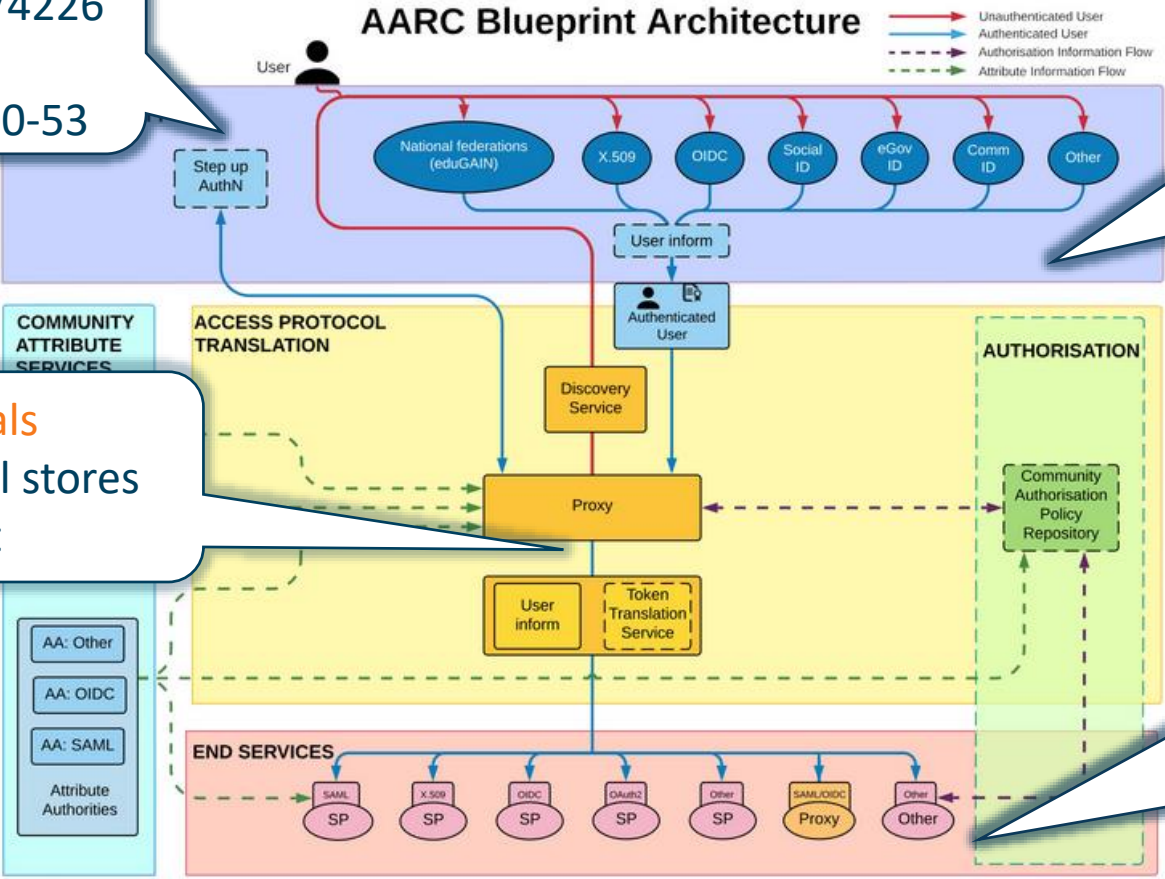
MFA
 RFC6238/4226
 FIPS140
 NISTSP800-53

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

Ephemeral credentials

- trusted credential stores
- protection at rest

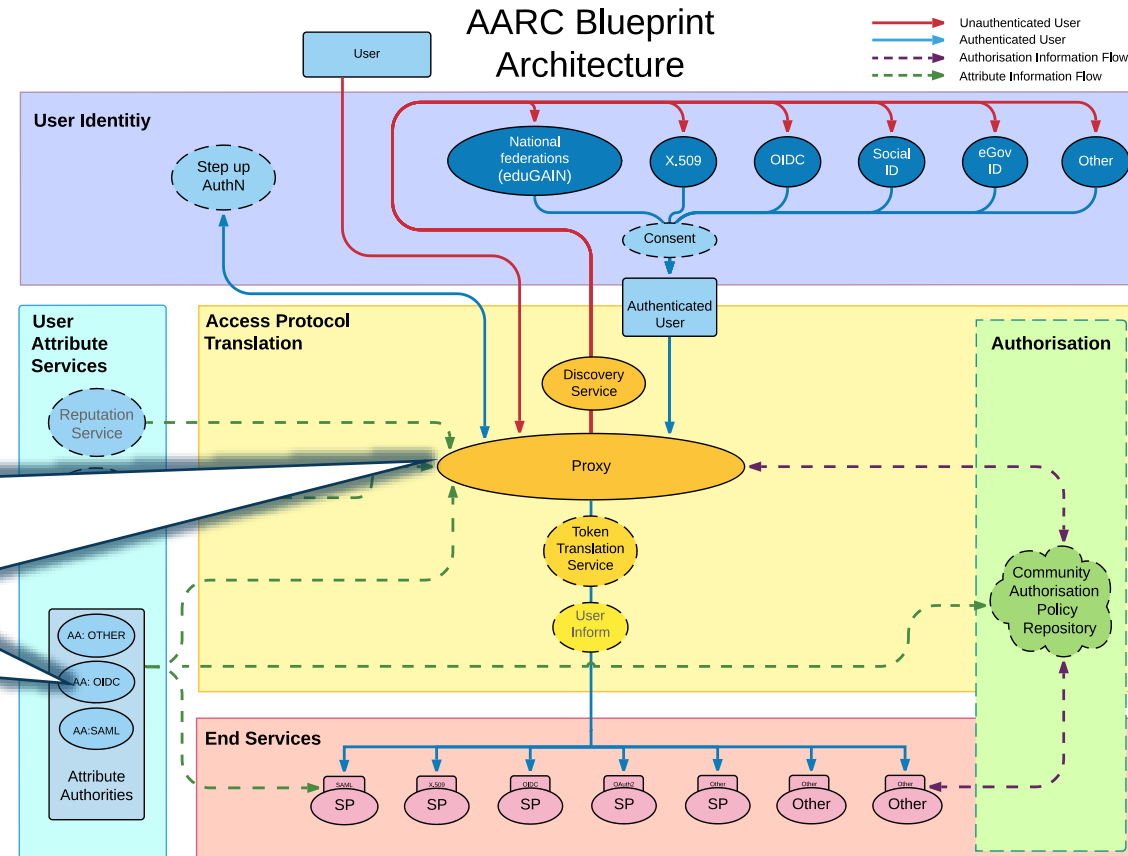
Service provider operations
 ISO27k
 Sirtfi
 Infrastructure response plans



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-1048, in collaboration with IGTF AAOPS)

AARC-G048: keeping users & communities protected, moving across models

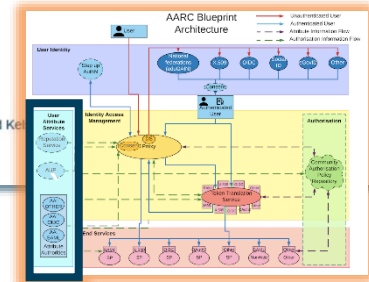


trusted delegation of response from communities to operators, and from services to communities in recognizing their assertions

Structured around concept of “**AA Operators**”, operating “**Attribute Authorities**” (technological entities), on behalf of, one or more, **Communities**

Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements

Publication Date: 2018-11-22
Authors: David Groep, David Ke Paetow, Maarten Kremers
Document Code: AARC-G048



3.3. Attribute Assertions

1. Assertions provided by an AA must be integrity-protected. They must be signed by the identified AA, or be transmitted over an integrity-protected channel where the server has been authenticated, and preferably both.

Push model

Where the protocol supports it, enable protection also of the messages conveyed over the established channel.

Good examples: SAML Attribute Query should enable message signing and use TLS.

Pull model

As a good example: LDAP should enable TLS protection of the channel

3.4.1. Key Management

1. A key used to protect assertions should be dedicated to assertion protection functions.

Push model

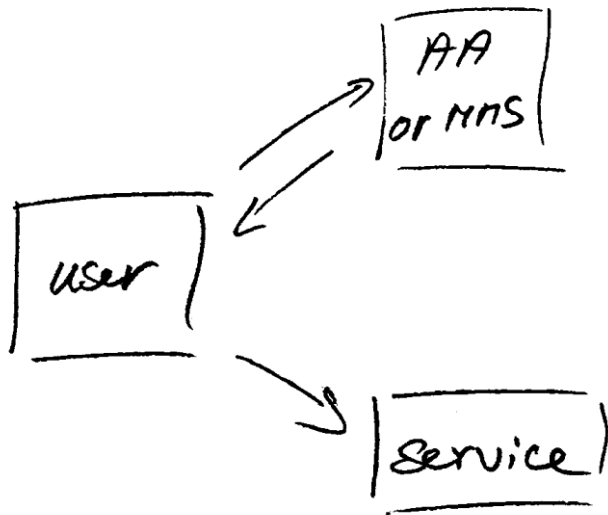
If the AA both signs assertions and provides functionality over protected channels, the keys used to sign assertions shall be different from those protecting those channels.

Pull model

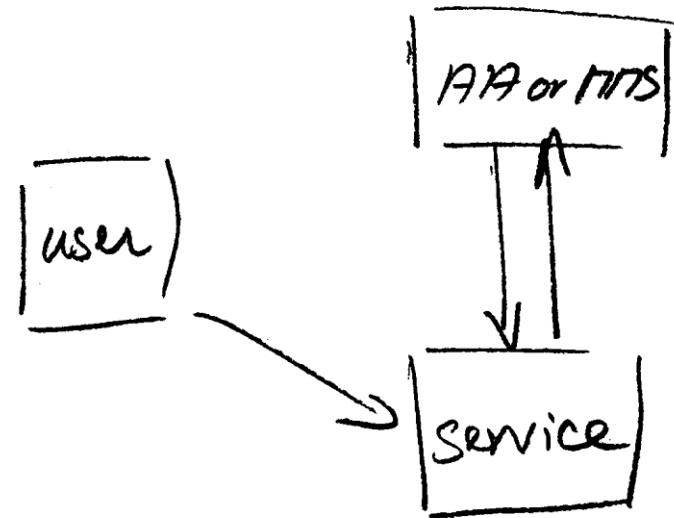
The key of the AA must be used solely for protecting connections to its protocol endpoint and ensure an integrity protected and mutually authenticated channel.

Protecting the community membership data and its proxy

Intentionally targeted broader than just BPA-style communities, since operational security spans data centres and infrastructures using other forms of AA membership management



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



*pull model – common when using directories
(e.g. LDAP in PRACE, GUMS in OSG)*

Deployment guidance included ...

1. Assertions provided by an AA must be integrity-protected. They must be signed by the identified AA, or be transmitted over an integrity-protected channel where the server has been authenticated, and preferably both.

Push model

Where the protocol supports it, enable protection also of the messages conveyed over the established channel.

Good examples: SAML Attribute Query should enable message signing and use TLS.

Pull model

As a good example: LDAP should enable TLS protection of the channel

6. The network to which the AA system is connected must be highly protected and suitably monitored.

Service access should be protected by at least two distinct control layers not running the same software or operating system, and the AA system must not run any unnecessary services. The network should be monitored for anomalous events, such as detection of data exfiltration, credential probing, and brute-force attacks. It should preferably also be protected

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 follow ought to be those that have been documented

But some items contain specific values and recommendations that are good practice, but where best practice varies among constituencies

Forward looking and specific requirements

Controls that are specific to AA operations and protect against current and future threats

- minimum signing key length so that the community is not broken in the next few years (at least 112-bit symmetric, i.e. ≥ 2048 bit RSA keys)
- protect the key from data breaches, compromise, ransomware, and exfiltration by using HSM Hardware Security Modules or equivalent controls (and the HSMs you need are not that expensive, or you can even rent them in AWS...)

Or deal with commensurate incident response (you don't want just a big red button):

- re-issuance of attribute statement must be based on fresh data
- release them only in accordance with the community's policy and maximum life time
- require appropriate client authentication before releasing attributes to prevent data breaches
- for non-revocable tokens (like OAuth Access Tokens or PKIX 3820 proxies), limit life time < 24 hrs (for OIDC, these are anyway typically 15 minutes)

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 should aim to fit 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. Our peer-review self-assessment model may be of specific value here

<https://wiki.geant.org/x/-YVgBw>

https://docs.google.com/document/d/1-hbqSpQegm7UaC_wupFzFMm19Q024UPkG-8Jwokkmzc

Thank you

Any Questions?

dauidg@nikhef.nl



<https://aarc-community.org>

