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

Publication Date	2022-02-24
Authors:	Members of the IGTF and the AARC Community; David Groep; Ian Collier, Tom Dack; Jens Jensen; David Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah Short; Mischa Sallé; Uros Stevanovic
With feedback from	Marina Adomeit; Sander Apweiler; Jim Basney; Christos Kanellopoulos; Johannes Reetz
AARC Document Code:	**AARC-G071**
Supported by:	*This guideline is a joint work of the International Global Trust Federation IGTF, the AARC community, and global partners. The research leading to these results has received funding from the European Community's Horizon2020 Programme by way of the AARC2 project (Grant Agreement No. 730941), EOSC-hub (Grant Agreement 777536), as part of the GÉANT 2020 Framework Partnership Agreement (FPA) under Grant Agreement No. 856726 (GN4-3), as well as from other sources*
Publishing Organisations:	IGTF and AARC Community
DOI:	https://doi.org/10.5281/zenodo.5927799

Abstract

These guidelines describe the minimum requirements and recommendations for the secure operation of attribute authorities and similar services that make statements about an entity based on well-defined attributes. Adherence to these guidelines may help to establish trust between communities, operators of attribute authorities and issuers, and relying parties, infrastructures, and providers. This document does not define an accreditation process.

Table of Contents

1. About this Guideline

These guidelines describe the requirements and recommendations for secure operation of attribute authorities, attribute aggregators and proxies, and of similar services that make statements about an entity based on well-defined attributes. Common scenarios include services that organise community membership management, 'proxies' as described in the AARC Blueprint Architecture [AARC-BPA] that collate or transform attributes, and membership directories – herein all referred to as 'Attribute Authorities'.

Associating attributes to entities (be they persons, identities in general, or themselves groups or roles) may be done in a variety of ways. Similarly, the conveyance of these attributes, and their binding to entities, varies depending on the architectural model of the authentication and authorization system. Yet regardless of the model chosen, trust placed in the attributes relies on the operational security integrity of the attribute authority that manages them. The guidance in this document concerns:

- operational security processes and procedures for attribute authorities that provide for an appropriate baseline information security practice,
- requirements on traceability, auditability, and logging that ensure operational security events involving attribute authorities can be analysed and mitigated,
- requirements on the secure (integrity-protected and confidential) operation of the attribute authority service itself and its service components, and
- requirements on securing the (integrity-protected and confidential) interactions with the attribute authority.

The latter two elements are partially dependent on the architectural model chosen for the authoritative attribute source. This document therefore distinguishes technology profiles for attribute authorities that:

- permit binding of properties to entities by means of lookup in which the entity whose properties are sought is the key in the look-up ('pull model')[1]
- issue (usually integrity-protected and, optionally, confidentiality-protected) statements in which attributes are asserted ('push model')[2]

Both models are discussed in the "Best Practices for managing authorisation" [AARC-G006]. Where guidance in this document is specific for one of these technology profiles, such requirements are indicated by being enclosed in profile-specific text boxes. Such guidance then applies only to that technology profile. Guidance that does not have such indication applies to all technology profiles, both pull- and push-based attribute authorities.

[1] Examples of the 'pull model' include the use of an LDAP directory queried by one or more access control decision points, either directly or through referrals, or a web service look-up such for an OIDC UserInfo endpoint..

[2] Examples of the 'push model' include issuing authorities that hand out signed attribute statements that can be presented to an access control system, such as used in the Virtual Organisation Membership Service VOMS by means of embeddable attribute certificates, the SAML assertions in a SAML2Int federation, or JWT tokens in an OAuth2 scenario.

The storage and processing of re-usable credential data (for instance to authenticate against the AA) is outside the scope of this document, but should comply with relevant credential issuer guidance.

In this document, the key words must, must not, should, should not, required, shall, shall not, recommended, may, and optional are to be interpreted as described in RFC 2119. If a 'should' or 'should not' is not followed, the reasoning for this exception should be documented and the AA Operator should disclose such to any affected parties so that they can evaluate the impact of thereof.

2. Definition of Terms

Community A set of one or more groups and sub-groups of persons (Users), organised with a common purpose and that are jointly granted access to one or more Infrastructures.

Community Management
A management body responsible for the Community and all its sub-groups, and for managing the lifecycle of user membership.

Attribute Authority (AA)
An attribute authority is a technical unit controlled by an organisation (such as a Community or infrastructure) that is entitled to make certain statements about entities, and assign attributes to them.
The AA may be the authoritative source of these statements, or be a proxy that asserts these statements based on trusted information it obtains from other sources. The assertions carrying these statements are generated by the technical service of the AA Operator.

AA Operator An organisation, a group of organisations under single administrative control or working under a single operational agreement for the purpose of AA Operations, or a group within an organisation, that runs one or more Attribute Authorities.

Attribute A named property associated with an entity. An attribute is controlled vocabulary that is semantically in common to both the Community and the Relying Parties who are supposed to interpret these attributes correctly.

Subject A subject is an entity for which the Community is able and entitled to make statements.

Attribute Assertion
A statement, made by the Attribute Authority, about the attributes of a subject, and which may include time of issuance, may include time of expiration, and may be signed.

Relying Party (RP)
A consumer of the attributes, who has to establish a trust relationship with the attribute authority.

3. Introduction

These guidelines describe the minimum requirements and recommendations for the secure operation of Attribute Authorities, and similar services providing statements for obtaining access to Infrastructure services.

In order to, for instance, make safe authorisation decisions, Relying Parties need to be able to identify and trust the issuer or provider of an attribute assertion, and know to which Community it pertains. In a typical scenario, a Community designates one or more AA Operators to operate AAs, and informs Relying Parties of any related metadata necessary for Pelying Parties to connect to or use the AA. The attributes are securely held by the AA and delivered on request to authorised Relying Parties, either directly or by way of the user. These attributes may be aggregated with identity assertions, such as delivered from a directory or group management system, or with attribute or capability tokens as asserted by an AARC BPA Proxy.

Stated compliance with these guidelines may help to establish trust between the Community and its AA, and Relying Parties. In the interest of scalability, these guidelines are intended to facilitate the assessment of AA Operators rather than individual AAs or Communities. This document does not provide guidance on the management (life cycle, technical implementation, exchange protocols etc.) of attributes nor the processes by which attributes are entered into the AA.

This document contains both normative as well as explanatory text. Normative guidance is labelled “YY-n”, and typeset in a coloured box for visual identification.

4. Operational Guidelines

4.1. Naming

Attributes are used both for authorization decisions (in access control policies) and for identifying ownership of stateful resources (files in a storage system for instance). Since their persistence in Relying Party systems is outside the control of the AA or AA operator, any re-assignment or relinquishing of name ownership will put user data and Relying Parties at risk. Hence, the names identifying the Communities and the AAs should be non-reassigned and globally unique. The intent is to prevent the identifier to be taken by a different organisation (either by chance or intentionally). This would then thereby result in confusing or incorrect attributes being accepted by Relying Parties.

AN-1

Identifiers of the AA Operator and the AA must both be non-reassigned and globally unique. In addition, the identifier of the Community should be unique. Identifiers should be chosen in accordance with the AARC Guidelines and the Community Membership Management policy [AARC-G003]. The AA must use a defined naming scheme for subjects and attributes. Subject identifiers must be non-reassigned and unique within an AA.

In case names whose semantics do not guarantee uniqueness are used (e.g. while URNs are guaranteed to be persistent, names in the domain name system could be re-assigned if they are inadvertently relinquished), the AA Operator and the AA must make a determined effort to impose such uniqueness. For example, domain name registrations must not be allowed to lapse, and a mechanism to ensure registration renewal in the future should be in place (e.g. by using subdomains under a long-lived organization, and not using project domain names unless due organizational care is taken, and the organisation managing the domain name has the intention of curating that domain name for a practically indefinite amount of time).

Push model implementation examples
Issued assertions must contain the community (AA) name embedded in the assertion (although where that may be, as part of the attribute, in an issuer claim, or otherwise, depends on technology and other applicable guidance). Where possible, the community name should be chosen as AA identifier, and should be the same as the “scope” domain name component as used in the assignment to identifiers of community users and in the naming of community attributes in the “Guidelines and the Community Membership Management policy” [AARC-G003]. For AA operators that provide a multi-tenancy service for communities created ad-hoc, the naming may be based on an identifier assigned to the AA operator and then further specialized. Some assertion models have the ability to contain independently both the AA operator name (issuer) and the AA name (authoritative). For such systems, both elements must be unique and persistent. E.g. for the VOMS system, the AA operator name shall be the issuer of the attribute certificate (a *directoryName* assigned or delegated by an independent authority such as the IGTF, or ISO/ITU-T) and the attribute authority name based on the scope element as described in AARC-G003.

Pull model implementation examples

For attributes that are looked up by the Relying Party, the identifier the RP will have is the one from the AA operator: typically the directory service end-point URL. It is recommended that the identifier persistency of the AA operator is also ensured through solely the domain name component of the URL. That is, the domain name used for the services by the AA operator must never be relinquished and remain tied to the AA operator.
 	
Good example:
`ldaps://ldap.surf.nl/ou=xenon,dc=co,dc=biggrid,dc=nl`
 	
Bad example:
`ldap://ec2-54-247-51-111.eu-west-1.compute.amazonaws.com:3389/o=beauty-vo`

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 publish documents defining the attribute set and the semantics used by the community, for the benefit of Relying Parties.

The AA Operator may be the only interaction point that the Relying Parties will know about, and thus the only way for them to gain insight into the Community policies and practices and thus evaluate the level of reliance to place in the attributes obtained. This can be as simple as providing a link back to a community information page, and may be implicit in case a community is created on a shared service platform.

AMR-4
The AA must only issue assertions or release attributes in accordance with the policies that are applicable to the Community.

AMR-5
When a community engages multiple AA Operators or operates multiple AAs, the community must ensure that the assertions issued are consistent between all issuers.

AMR-6
The community should ensure that within one assertion issued attributes are consistent.

4.3. Attribute Assertions

AAS-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.

In a push model, where the protocol supports it, the AA and RP should enable both confidentiality and integrity protection of the assertions conveyed over the established channel (by signing or encrypting the assertions, or both). For instance, a SAML Attribute Query should enable message signing and use TLS.

In a pull scenario, TLS protection of the channel should be used for all queries.

AAS-2

In addition to meeting its own regulatory obligations, the AA must respect data protection requirements of the Community. It is recommended that AAs require client authentication, in addition to the encryption of the messages and the communication channel. The AA should not send more data than required by the RP.

In some pull cases, the client has an identity and a secret to authenticate with (e.g. a service credential to connect to a membership management service). In other cases, there is no such secret information available: e.g. in the OpenID Connect OIDC public client model [RFC6749], the protection put in place to prevent the client from retrieving arbitrary data from the OpenID Connect Provider (OP) is the introduction of an intermediate page at the user authentication point and asking agreement for attribute release from the user. This constitutes an implementation of ‘client authentication’ as intended in the clause above (by putting the user and client as equivalent, where the user has ‘registered’ the client with implicit trust in the software or service by the user). As a result, when using a public client, consent must be enabled.

In models where a trusted federation is in place, it may be replaced by this third-party trust model within the federation for its (by now confidential) client, depending on the specific use case and data protection requirements.

AAS-3

If an AA Operator issues assertions containing a lifetime, this lifetime must be compliant with the Community policies, as short as reasonably possible, and the assertion must not be valid beyond the validity period of the attributes it contains. The Community Management is responsible for the content of the assertion, as issued, during its entire lifetime.

These guidelines do not require a revocation mechanism for issued attribute assertions.

The bearer-token RFC6750 suggests short-lived (1 hour or less) tokens reduce the impact of them being leaked. In many OIDC scenarios, the typical validity is 15 minutes, and e.g. VOMS attribute certificates are valid for 12 hours by default. Nevertheless, some communities have chosen to extend that up to 72 hours for specific scenarios.

AAS-4
Re-issuance of assertions must be based on information held in the AA at the time of re-issuance.

While this is readily understood for any re-issuance where a completely new assertion is created, it is equally applicable in other re-fresh scenarios. For instance, when an OAuth2 RP is renewing a JWT with claims, the refresh token is validated by the issuer and *at that point* the AA can either issue a JWT, or not, or update the information therein, based on then-current information in the AA. The refresh tokens themselves are conceptually equivalent to user credentials and, as such, attribute issuers should follow guidance for identity issuing authorities when issuing refresh tokens.

4.4. Operational Environment

Securing the environment and its operations aims to prevent compromises from spreading between services and environments and thereby negatively impact the integrity and confidentiality of the AA service.

OE-1
Through its personnel or by contractual measures, the AA Operator should ensure appropriate controls are in place over the security context.

OE-2
The AA must be located in a physically secure environment where access is controlled and limited to specific trained personnel.

OE-3
The protections on the AA and its operational environment, including the credentials of the AA administrators and operators, should meet or exceed the requirements of all of the communities hosted in the AA.

Implementers of AAs should use placement policies to ensure physical and/or virtual separation of sensitive and non-sensitive services, containers, or virtual machines, to reduce the risk of cross-compromise. In all cases, the environment itself must be protected according to current best practice, and a risk assessment of the environment should be performed [e.g. based on the WISE SCI [SCI] and Sirtfi [SIRTFI] requirements], taking into account both the integrity of the AA as well as the requirements of the communities hosted on the AA and the Relying Parties receiving attributes.

4.5. Key Management

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

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

If the assertions conveyed over the channel are to be independently protected, this protection should then use another key.

Pull model
The key used for protecting connections to the AA's protocol endpoint must be a dedicated key ensuring a protected and authenticated channel.

KM-2

Keys must not be shared between AA Operators. A single AA Operator may use the same signing key for multiple AAs. Where multiple AAs are under the control of a single AA operator but located in physically distributed locations, the key must only be transported using secure protocols.

For example, an AA Operator can be physically distributed but still constitute a single 'organisation' if there is a common managerial control over all distributed instances. It must then have a single operations coordination team, which is under single management. This is one operator. Key distribution must in this case be controlled by a protocol that protects against compromise in transit and at rest. Where a community commissions multiple operators (that are not under common management) to run their AA, each operator must use different keys to allow RPs to differentiate between them.

KM-3

Keys must have a protection strength equivalent to 112 bits[3] (symmetric) or higher.

To compare key strength between different mechanisms, refer to, *e.g.*, NIST Special Publication 800-57 Part 1 [SP800-57-1] on key management. Cryptographically, 112-bit symmetric encryption is equivalent to 2048-bit RSA, 128-bit encryption to 3072-bit RSA or 256- to 383-bit ECC. Anything above that (e.g. 192 symmetric bits) is hard to express in workable RSA keys (8192-bit and larger), and should preferably be protected through ECC.

KM-4

Keys must only be accessible by the service and by trained personnel subject to procedural controls.

KM-5

AA Operators are recommended to use an HSM to store signing keys.
When using software-based private keys, such keys must be suitably protected by the operating system. Keys should not be held unencrypted on persistent storage protected solely by database, storage and file system level permissions.

When keys are not stored in an HSM, they should exist in activated form in memory only (and key daemon mechanisms may be employed in high-availability environments to maintain service continuity by key re-synchronisation).

4.6. Network Configuration

[3] The reference value 112 applies to adequate protection as of 2022. The appropriate value may increase over time.

NET-1

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 against denial of service attacks in order to prevent security downgrade attacks and fail-overs that are induced unexpectedly.

4.7. Site Security

SITE-1

The AA Operator must ensure appropriate site security controls are in place and maintained in a state consistent with the security requirements of the hosted Communities.

For example this can be based on contractual agreements, available audits of the site security controls of a provider, or on actual control and inspections, e.g. the system is in a locked room with auditable physical access controls, protected against intrusions and be at least tamper-evident in case of such intrusions.

Additional elements such as flood and fire protection, or protection against threats emerging as a result of providing service to specific communities, should be considered as well.

4.8. Metadata Publication

MD-1

The AA Operator must publish, to the Community and related Relying Parties, at least the following metadata for each AA it hosts:

(a) administrative contact details for the AA Operator, including at least one role-based email address and one postal contact address,

(b) an operational security contact for the AA Operator, being at least a role-based email address but preferably including a telephone number,

(c) cryptographic key material required to verify signed messages, where that is required to validate issued attribute assertions.

The operational security contact is expected to respond in a manner consistent with the *Sirtfi* requirements.

Role-based email addresses are preferred both to prevent releasing personal data to the public as well as to cater for people changing positions or leaving. For a postal address, this could e.g. be directed to a group secretariat. The postal address also establishes country and jurisdiction (which could be relevant to privacy notices).

MD-2

It is recommended that the AA Operator publishes, where available,

(a) such validated trust marks as are relevant to the evaluation of the security and trust of the AA by the Communities, Identity Providers, and Relying Parties;

(b) a (web) URL to a general information web page about the Community.

MD-3

The AA Operator should provide a means to validate the integrity of its roots of trust.

For instance, validating the integrity of trust roots can be done by submitting them to a trust anchor repository such as a national federation or eduGAIN metadata aggregate, the IGTF trust anchor distribution, the trust anchor distribution of a pertinent e-Infrastructure, or the set of public web trust roots.

4.9. Assessment and Review

AR-1

The attributes in the AA and their binding to subjects must be verifiable and assessable.

The AA should attach supplementary attributes based on a managed source of data - such as a corporate directory, or a community membership database that is kept up-to-date - that is auditable, or on predictable transformation of incoming data.

AR-2

The AA Operator must log, for the purpose of traceability in support of security incident response, where the AA provides relevant attributes, at least the following for all of its hosted AAs:

(a) all requests for attributes and all issued attribute assertions, to the extent that they are needed to allow traceability of attribute release to individuals during incident response by receiving qualified Relying Parties;

(b) any configuration change to the AA relevant to the access control of the attribute repository;

(c) any change affecting the binding between subjects and attributes.

The AA Operator, in its published privacy and confidentiality policies must permit logging as required above.

The traceability can be obtained even when retaining only opaque identifiers, when such can be used in conjunction with upstream data (typically, from the user's institutional identity provider) to identify individual actions.

AR-3 The AA Operator must log at least the following for its AA issuance systems, for the purposes of incident response: (a) all login, logout, reboot, and key activation events of the issuing system; (b) changes to the configuration of the issuing system.
AR-4 The AA Operator must keep records regarding attribute release and its issuance systems after termination of the effects of the auditable events for as long as required by the Community and any Relying Parties that have entered into an agreement with the AA Operator, and as required by applicable legislation.

The retention period should be agreed with both Relying Parties and the hosted communities. There may also be regulatory requirements governing minimum retention periods. Typical guidance for retention periods are 180 days (response to immediate IT security incidents), 398 days (13 months) based on an annual employment-, study-, or credential issuing life cycle, or anywhere between five years and seven years (e.g. in a banking or fiscally-regulated environment).

AR-5 The AA operator must disclose and discuss, on request, those aspects of their operational environment that are relevant to the evaluation of the security and trust by the Communities and Relying Parties.
AR-6 The AA Operator must be able and willing to collaborate with affected organisations in the management of a security incident.
AR-7 The AA Operator should review roles, rights, and access of its staff at least once per year.

4.10. Privacy and Confidentiality

PC-1 The AA operator must define and publish a privacy and data release policy, and that policy must be compatible with the assertions that it issues, and be compliant with relevant legislation.

A community can only use an AA operator if its community policy is compatible with the policies of the AA. Yet there is also a benefit for the Relying Parties in the AA facilitating access to the community privacy policies, and clearly also the AA operator must review the community privacy policies for compatibility with its own policies.

Who is responsible for the data (in the context of GDPR the Data Controller) depends on the relationship between the community (or its legal entity) and the AA operator, and their contractual relationship.

Depending on the role of the AA Operator in the relationship, it may provide appropriate privacy policy templates to the communities it supports, or mandate a specific policy.

4.11. Business Continuity and Disaster Recovery

BCDR-1 The AA Operator must have a compromise and disaster recovery procedure, and a business continuity plan.
BCDR-2 The business continuity and disaster recovery plan must be compatible with the requirements of the hosted Communities.

In addition, the Relying Parties can require a disaster recovery and continuity plan, since in incident response for instance they will need the participation of the AA operator and the community in order to provide traceability.

5. Relying Party Obligations

RP-1 Relying Parties must, at the time of reliance, verify the integrity and validity of attribute assertions and any binding to a valid subject, to their satisfaction.

If the time of reliance is shifted from the time of receipt of the assertion, e.g. in case of batch processing, the Relying Party should still verify the validity of any expired assertions by refreshing these at the time actions are taken.

RP-2 Relying Parties must rely on assertions with an explicit lifetime only during their validity period.
RP-3 Relying Parties must assess the risk of relying on assertions with no explicit lifetime and should not rely on them for longer than the relevant industry standards for that type of assertion recommend[4].

The relevant validity period highly depends on the type of token or assertion. For some forms of attribute certificate, this could be six to 24 hours. For other types, such as bearer tokens, it can be as short as 15 minutes. For a directory based look-up (in a pull model), it should be checked every time and the result should probably not be cached longer than approximately 10 minutes (the typical Unix name-service cache period).

RP-4 Any long-lived, non-revocable statements received from an AA must be appropriately protected for confidentiality and integrity, by proxies and other intermediate entities.

[4] neither the AA Operator nor the AA are responsible for decisions based on information without a specified lifetime after the AA has updated its own database

References

AARC-BPA *AARC Community, N. Liampotis (ed.)*, “AARC Blueprint Architecture 2019”, AARC-G045, https://doi.org/10.5281/zenodo.3672784

AARC-G006 *AARC Community*, “Best Practices for managing authorisation”, AARC-G006, https://aarc-community.org/guidelines/aarc-g006/

EPSC REFEDS schema working group, “eduPerson Schema”, https://refeds.org/eduperson

RFC6749 D. Hardt (ed.) “The OAuth 2.0 Authorization Framework”, RFC 6749, https://tools.ietf.org/html/rfc6749 (herein specifically section 2.1)

SCHAC REFEDS schema working group, “Schac: Schema for Academia”, https://refeds.org/schac

SIRTFI REFEDS Sirtfi working group, “Security Incident Response Trust Framework for Federated Identity (Sirtfi)”, https://refeds.org/SIRTFI

SP-800-57-1 National Institute for Standards and Technology, “NIST Special Publication 800-57 Part 1 – Recommendations for Key Management, Rev 5”, NIST, 05/2020, via https://csrc.nist.gov/projects/key-management/key-management-guidelines (visited January 31, 2022)

WISE WISE Information Security for E-infrastructures Security for Collaborating Infrastructures working group, “WISE SCI Trust Framework v2”, https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

Acknowledgements

This Guideline is based on work by the Interoperable Global Trust Federation and the AARC Authentication and Authorization for Research Collaboration community, and is derived from the AARC Guideline G048, published in 2018 (https://doi.org/10.5281/zenodo.3234926).

It has been extensively reviewed and extended since, based on review by members of the AARC Engagement Group for Infrastructures (AEGIS), whose comments have significantly clarified and generalised the guidelines. The authors would like to thank Marina Adomeit (SUNET and GEANT), Sander Apweiler (Forschungszentrum Jülich and EUDAT), Jim Basney (National Center for Supercomputing Applications at the University of Illinois Urbana-Champaign, and CILogon), Christos Kanellopoulos (GEANT), and Johannes Reetz (RZG Max Planck Society and EUDAT) for their clarifying comments and feedback.

We would also like to acknowledge the discussion and contributions during the formative and rather extended period of this document, during which participants in the plenary IGTF sessions have commented and discussed on the topic of authorisation and attribute trust.

The research leading to these results has also received funding from the European Community's Horizon2020 Programme by way of the AARC2 project (Grant Agreement No. 730941), from EOSC-hub (Grant Agreement 777536), and from the GÉANT 2020 Framework Partnership Agreement (FPA) under Grant Agreement No. 856726 (GN4-3).