Attribute Authority and Proxy operational security

Associating properties to entities (be they persons, identities in general, or themselves groups or roles) may be done in a variety of different ways. Similarly, the conveyance of these properties, 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 authority that manages them. The guidance is intended to help attribute authorities but also operators of other proxy elements in the AARC Blueprint Architecture that manage sensitive credential data with appropriate management and operational security practices.

Some elements are (partially) dependent on the architectural model chosen for the authoritative attribute source. This document therefore distinguishes technology profiles for attribute authorities: (i) 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') and (ii) attribute authorities that issue (usually integrity-protected and, optionally, confidentiality-protected) statements in which attributes are asserted ('push model')

Revision 2 "AARC-G071" for review by the (AEGIS) Infrastructures

Guideline 071 (previously known as **G048bis**) evolved and clarifies the scope of the guidance for Attribute Authority operators. Specifically, we realise that the AAOPS guidelines are applicable not only to the membership management services, but are equally relevant for the other proxy components. In the revision process, we look at generalising the guidance so that attribute-specific elements are removed and more flexibility is added to cater do the various proxy delivery models (as-a-service, bespoke, multi-tenant, and on-prem).

Comments and suggestions to this pre-publication were invited from the AARC Community policy community and the IGTF, and endorsed by AEGIS on April 11th, 2022:

- AARC-G071Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities (OfficeXML document)
- Official publication in Zenodo (https://doi.org/10.5281/zenodo.5927799) also here as PDF document

The document above has been consolidated from the Google document that had received feed-back in 2021. That version has been re-formatted for readability, and an acklowledgement section and list of authors and contributors has been added to it. The Google document, and its comment history, are preserved here:

- (depricated) Commentable document in Google docs

The work is run in the AARC Policy Area with additional contributions from all AEGIS members. The public consultation ("AEGIS v2") version was finalised in the 54th EUGridPMA+ meeting in January 2022

Latest public (formatted) version

- AARC-G048 in OfficeXML format
- AARC-G048 in PDF format
- Guidelines page on the AARC community website

Supporting material:

- Assessment sheet

Associating properties to entities (be they persons, identities in general, or themselves groups or roles) may be done in a variety of different ways. Similarly, the conveyance of these properties, 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 authority that manages them. The guidance is intended to help attribute authorities but also operators of other proxy elements in the AARC Blueprint Architecture that manage sensitive credential data with appropriate management and operational security practices.

Some elements are (partially) dependent on the architectural model chosen for the authoritative attribute source. This document therefore distinguishes technology profiles for attribute authorities: (i) 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') and (ii) attribute authorities that issue (usually integrity-protected and, optionally, confidentiality-protected) statements in which attributes are asserted ('push model')

Revision 2 "AARC-G071" for review by the (AEGIS) Infrastructures

Guideline 071 (previously known as **G048 revision 2**) evolved and clarifies the scope of the guidance for Attribute Authority operators. Specifically, we realise that the AAOPS guidelines are applicable not only ot the membership management services, but are equally relevant for the other proxy components. In the revision process, we look at generalising the guidance so that attribute-specific elements are removed and more flexibility is added to cater do the various proxy delivery models (as-a-service, bespoke, multi-tenant, and on-prem).

Comments and suggestions to this pre-publication are invited from the AARC Community policy list, AEGIS, and the IGTF - at this stage by email to the authors or comments to this Wiki page:

- AARC-G071Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities (OfficeXML document)
- Pre-publication also as PDF document

The document above has been consolidated from the Google document that had received feed-back in 2021. That version has been re-formatted for readability, and an acklowledgement section and list of authors and contributors has been added to it. The Google document, and its comment history, are preserved here:

- (depricated) Commentable document in Google docs

The work is run in the AARC Policy Area with additional contributions from all AEGIS members. The public consultation ("AEGIS v2") version was finalised in the 54th EUGridPMA+ meeting in January 2022

Latest public (formatted) version

- AARC-G048 in OfficeXML format
- AARC-G048 in PDF format
- Guidelines page on the AARC community website

Supporting material:

- Assessment sheet

Associating properties to entities (be they persons, identities in general, or themselves groups or roles) may be done in a variety of different ways. Similarly, the conveyance of these properties, 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 authority that manages them. The guidance is intended to help attribute authorities but also operators of other proxy elements in the AARC Blueprint Architecture that manage sensitive credential data with appropriate management and operational security practices.

Some elements are (partially) dependent on the architectural model chosen for the authoritative attribute source. This document therefore distinguishes technology profiles for attribute authorities: (i) 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’) and (ii) attribute authorities that issue (usually integrity-protected and, optionally, confidentiality-protected) statements in which attributes are asserted (‘push model’)

Revision 2 "AARC-G071" for review by the (AEGIS) Infrastructures

Guideline 071 (previously known as **G048 revision 2**) evolved and clarifies the scope of the guidance for Attribute Authority operators. Specifically, we realise that the AAOPS guidelines are applicable not only ot the membership management services, but are equally relevant for the other proxy components. In the revision process, we look at generalising the guidance so that attribute-specific elements are removed and more flexibility is added to cater do the various proxy delivery models (as-a-service, bespoke, multi-tenant, and on-prem).

Comments and suggestions to this pre-publication are invited from the AARC Community policy list, AEGIS, and the IGTF - at this stage by email to the authors or comments to this Wiki page:

- AARC-G071Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entitiesAARC-G071-Secure-Operation-of-Attribute-Authorities-PUB-20210202.docx(OfficeXML document)
- Pre-publication also as PDF document

The document above has been consolidated from the Google document that had received feed-back in 2021. That version has been re-formatted for readability, and an acklowledgement section and list of authors and contributors has been added to it. The Google document, and its comment history, are preserved here:

- (depricated) Commentable document in Google docs

The work is run in the AARC Policy Area with additional contributions from all AEGIS members. The public consultation ("AEGIS v2") version was finalised in the 54th EUGridPMA+ meeting in January 2022

Latest public (formatted) version

- AARC-G048 in OfficeXML format
- AARC-G048 in PDF format
- Guidelines page on the AARC community website

Supporting material:

- Assessment sheet

Associating properties to entities (be they persons, identities in general, or themselves groups or roles) may be done in a variety of different ways. Similarly, the conveyance of these properties, 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 authority that manages them. The guidance is intended to help attribute authorities but also operators of other proxy elements in the AARC Blueprint Architecture that manage sensitive credential data with appropriate management and operational security practices.

Some elements are (partially) dependent on the architectural model chosen for the authoritative attribute source. This document therefore distinguishes technology profiles for attribute authorities: (i) 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’) and (ii) attribute authorities that issue (usually integrity-protected and, optionally, confidentiality-protected) statements in which attributes are asserted (‘push model’)

Revision 2 "AARC-G071" for review by the (AEGIS) Infrastructures

Guideline 071 (previously known as **G048 revision 2**) evolved and clarifies the scope of the guidance for Attribute Authority operators. Specifically, we realise that the AAOPS guidelines are applicable not only ot the membership management services, but are equally relevant for the other proxy components. In the revision process, we look at generalising the guidance so that attribute-specific elements are removed and more flexibility is added to cater do the various proxy delivery models (as-a-service, bespoke, multi-tenant, and on-prem).

Comments and suggestions to this pre-publication are invited from the AARC Community policy list, AEGIS, and the IGTF - at this stage by email to the authors or comments to this Wiki page:

- AARC-G071Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities (OfficeXML document)
- Pre-publication also as PDF document

The document above has been consolidated from the Google document that had received feed-back in 2021. That version has been re-formatted for readability, and an acklowledgement section and list of authors and contributors has been added to it. The Google document, and its comment history, are preserved here:

- (depricated) Commentable document in Google docs

The work is run in the AARC Policy Area with additional contributions from all AEGIS members. The public consultation ("AEGIS v2") version was finalised in the 54th EUGridPMA+ meeting in January 2022

Latest public (formatted) version

- AARC-G048 in OfficeXML format
- AARC-G048 in PDF format
- Guidelines page on the AARC community website

Supporting material:

- Assessment sheet