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 BPA model 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')

The storage and processing of re-usable credential data is outside the scope of this document, but should comply with relevant credential issuer guidance. Storage and processing of such data is strongly discouraged.

This work is performed also in the context of the EUGridPMA and IGTF Attribute Authority Service Operations guidelines, where the future evolution of this document after the end of the AARC project will continue

Latest public (formatted) version

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

Revision 2 - commentable version for review by the (AEGIS) Infrastructures

Guideline 48 revision 2 (initiated February 2020) will evolve and clarify the scope of the guidance for Attribute Authority operators. Comments and suggestions to revision 2 are invited by email to the AARC Community policy list and as comments to the collaborative document here:

- Commentable document in Google docs

Supporting material:

- Assessment sheet