Authorization Information Format (AIF)

draft-bormann-core-ace-aif-09

Carsten Bormann

IETF 108

Problem: Convey authorization information

- Authorization ("Access Control") is usually modeled by the *Access Control Matrix* (Lampson 1971), a function mapping a Subject and an Object to a set of Permissions (Rights): M: S x O $\rightarrow 2^R$
- This is often sliced by object into an ACL (Access Control List)
- To know about the authorizations of a client, we slice by subject: "Capability list" or "C-list", C: O $\rightarrow 2^R$
- Binding to subject done outside, e.g. in access grant (in certain kinds of secure channel, or providing some subject authentication verifier, e.g., a Proof of Possession token)

draft-bormann-core-ace-aif

- Represent C-list as an array of pairs:

  AIF-Generic<Toid, Tperm> = [* [Toid, Tperm]]

- For the RESTful case, specialize to:

  AIF-REST = AIF-Generic<path, permissions>

  path = tstr *; URI relative to enforcement point — O*

  permissions = uint .bits methods ; *what methods are allowed* — 2^R

  methods = &(GET: 0 POST: 1 PUT: 2 DELETE: 3 FETCH: 4 PATCH: 5 iPATCH: 6)

- Could define other cases, e.g., for MQTT (outside scope of this spec)

Dynamic permissions in draft-bormann-core-ace-aif-09

- AIF is designed for static resources of IoT devices
- Actions often lead to dynamic “action resources” (pointed to by Location-* response options)
- Idea: Derive permissions from base resource
- methods /= &(Dynamic-GET: 32 Dynamic-POST: 33 Dynamic-PUT: 34
  Dynamic-DELETE: 35
  Dynamic-FETCH: 36 Dynamic-PATCH: 37 Dynamic-iPATCH: 38)
- These permissions say what can be done to resources created from the resource to which they apply (a bit like NFSv4 inheritance)

Status for draft-bormann-core-ace-aif-09

- AIF has been around since 2014 (part of DCAF work);
  was listed as contribution on ACE BOF at IETF 89
- ACE has recently noticed a need to go ahead with standardizing this;
  WG adoption call ends today (**you can still put in your opinion**!)
  - Ben Kaduk:
    What else exists like this? How could AIF be used outside ACE?

- On agenda of ACE meeting tomorrow