Discovery for BRSKI
draft-ietf-anima-brski-discovery-07
IETF123 Madrid
(was -05 at IETF121)

Toerless Eckert, Futurewei USA (tte@cs.fau.de)

Esko Dijk (esko.dijk@iotconsultancy.nl)

07/21/2025

Summary – changes since -05

- Very helpful reviews of Steffen Fries, Artur Hecker, initial review by Matthias Kovatsch

- Open issue: Artur suggesting to split up document
  - Claim: core is data-model, IANA registries
  - Could split out: a) transparent proxy behavior, b) Pledge IDdev details

  - Current author answer: goal of docuemnt is autoconfiguring, resilient, automatically extensible BRSKI operation – for arbitrary discovery protocols
    - The specs how to use discovery is the core – specificiation of a solution
    - Data model and IANA registries are just the (quite complex) dependencies to make solution simple
    - Improved text (abstract etc.) to make this hopefully more easily understood

Changes on wire an/or Registry

- Wire only
  - GRASP example was wrong.
  - Also expanded GRASPexamples to show both registrar and resulting proxy announcements. Also added more explanations.
    - Single GRASP message vs. multiple GRASP messages (per App GRASP implementation)
- Wire / registry
  - “cms” / “rrm-cms-est” -> “cmsj” / “rrm-cmsj-est” - “j” for JSON
    - Because we could get non-json encoding for for CMS variants of BRSKI
- Registry only
  - BRSKI context -> tBRSKI context (‘t’ for TCP)
    - cBRSKI is explicitly BRSKI over UDP. But what does BRSKI mean ? Everything together or just BRSKI over TCP ? New term makes it easier to distinguish.

Improvements in text

- Defined spec as update to draft-ietf-anima-brski-prm
  - Because of refinement, more SHOULD for DNS-SD encoding of IDevID for pledge discovery
- Rewrote Abstract to explain those goals (re. Artur)
- Expanded intro(“Challenges”)
  - Enumerate example deployment failures without discovery
- “See Section 1” – gave up on idea of references into terminology section
- “Terminology”
  - Unclear “IP” -> IPv6 + IPv4 = IP
  - Roles vs. Services: RFC8995 did not have “Roles”. But now we have variations “Registrar” is role, but “RFC8995 Registrar” is now a service (variation).
- Explicitly mentioning Agents as clients to discovery beside Pledges where applicable.
- Lots of duplicate text removal in variation agnostic proxy spec sections.

Improvements in text

- Add explanation why Pledge discovery currently only specified for DNS-SD
  - missing needs for the other discovery options – can be added reasonably easy.
- CA -> trust anchor
- Much reworked/improved Pledge discovery section
  - Description reworked into step-by-step bullet point list
  - Example accordingly re-structured as well
- New security considerations section about (in)security of discovery
  - Usually resolved by underlying network (domain) security
  - E.g.: ACP – RFC8994 or per-hop L2 security (mesh radio networks)
  - Or also just physcial access to transit hops considered to be hard enough (Enterprise).

Next Steps

- Get early review by IANA (large registry tables)
  - Sheng asked AD (Mahesh). Toerless also asked IANA directly
- Outstanding review from Liubing, discuss with Matthias
- Want to get another review by DNS-SD expert
- Planning to ask for WGLC for IETF124

Questions ?

- Thank you!