

Update on BRSKI with Pledge in Responder Mode (BRSKI-PRM)

[draft-ietf-anima-brski-prm-10](#)

Repo URL: <https://github.com/anima-wg/anima-brski-prm>

Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson

Shepherd: Matthias Kovatsch

IETF 118 – ANIMA Working Group

BRSKI-PRM Status

History of main changes 09 → 10

- Addressed remaining issues from WGLC (03/2023) and design team discussions.
- Most issues related to clarifications of terminology and call flow descriptions
- Technical issues clarified:
 - Included conflict resolution in mDNS and GRASP (Issue #93, Section 5.3.2)
 - Enhanced host header processing on pledge side (issue #120, Section 5.2)
 - Clarified availability of serial number information on domain registrar for pledge authorization (issue #122, Section 6.1)
 - Clarified usage of alternative voucher formats (issue #123, Section 6.2.3)
 - Removed strength comparison for voucher assertions (issue #125, Section 5.1 + 6)

BRSKI-PRM, Open Issue #79

Discovery of registrar with BRSKI-PRM feature set

- Discovery of registrar by and registrar-agent is not needed (have a trust relation and are assumed to exchange upfront information).
- Current discovery in BRSKI does not consider registrars with enhanced feature sets. This is handled in ID [BRSKI-Discovery](#).
- Proposal to keep simple assumption in BRSKI-PRM and refer to BRSKI-Discovery for cases, in which the enhanced discovery of a registrar by a registrar-agent is described (considering, e.g., the mode of operation or voucher formats)

BRSKI-PRM, Open Issue #130

Discovery of pledges by a registrar-agent

- Discovery of pledges by a registrar-agent using DNS-SD with mDNS in two ways:
 - "product-serial-number._brski-pledge._tcp.local", to discover a specific pledge.
 - "_brski-pledge._tcp.local" to discover available pledges for bootstrapping.
- ID [BRSKI-Discovery](#) describes more versatile approach to contain additional info (e.g., manufacturer) to product serial number but also to used, e.g., GRASP.
- Proposal to keep simple discovery in BRSKI-PRM by using manufacturer-specific product serial numbers and DNS-SD with mDNS as minimal solution to be supported and to refer to BRSKI-Discovery for enhanced discovery.
 - Note: May result in false positives (many manufacturer likely have serial number 001), the registrar-agent can filter through the results, e.g., based on the related IDevID CA certificate.

BRSKI-PRM Status

Next Steps

- Finalize open issues #79 and #130 (see [ANIMA git](#))
- WGLC done before IETF 116
- IOT DIR early review done
- SECDIR early review to be updated
- Shepherd writeup
- Ready for AD review
- Interop testing with others welcome 😊,
PoC implementations of all components available, please get in touch

Backup: BRSKI-PRM – Abstract Protocol Overview

