

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

[draft-ietf-anima-brski-prm-08](#)

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

Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson

Shepherd: Matthias Kovatsch

IETF 116 – ANIMA Working Group

BRSKI-PRM Status

History of main changes 05→ 06

- Issue #67, shortened the pledge endpoints to prepare for constraint deployments
- Included table for new registrar endpoints in section 5.3
- Addressed review comments from SECDIR early review (mainly editorial improvements)
- Addressed review comments from IOTDIR early review (Update of return codes in case of errors, terminology clarifications, consequent use of normative language, editorial improvements, update of references)

BRSKI-PRM Status

History of main changes 06→ 07 → 08

- WGLC resulted in a removal of the voucher enhancements completely from this document to RFC 8366bis, containing all enhancements and augmentations of the voucher, including the voucher-request as well as the tree diagrams
- Resolved editorial issues discovered after WGLC (still open issues remaining see next slide)
- Resolved comments from the Shepherd review as discussed in PR #85 on the ANIMA github (editorial, terminology alignments)

BRSKI-PRM Open Issues collected after WGLC

- #79 discovery of registrar with BRSKI-PRM function set
 - DNS-SD with subtypes or text parameters to distinguish different function sets
- #80 pledge discovery using GRASP?
 - Mention as alternative but ot-of-scope for the draft
- #81 Additional text to explain usage of agent-signed data
 - Text prepared for section 5.4 and for the introduction
- #82 Include text related to TLS library issues
 - Background: pledge cannot use IDevID as TLS server certificate as registrar-agent can't verify
 - Proposal: not to be addressed in the draft

BRSKI-PRM Open

Issues collected after WGLC (cont.)

- #83 Clarify re-enrollment support in BRSKI-PRM
 - BRSKI-PRM and BRSKI focus on bootstrapping and do not address re-enrollment
 - Text to be added to motivate use of existing endpoints for re-enrollment
- #84 use of registrar endpoints for responder vs. initiator mode
 - BRSKI-PRM assumes the registrar can distinguish LDevID (registrar-agent) vs. IDevID (pledge) also on existing endpoints → proposal to keep this handling
 - PRM specific Media Type naming proposed to allow for using the same endpoint with different media types (instead of decision based on *DevID)
- #86 pledge/registrar recognition based on credential
 - As in #84: BRSKI-PRM assumes the registrar can distinguish LDevID (registrar-agent) vs. IDevID (pledge) also on existing endpoints → proposal to keep this handling

BRSKI-PRM Status

Next Steps

- Address open issues (see [ANIMA git](#))
- Restructure section 5 and 6 for better readability and understanding
- Interop testing with others welcome 😊,
PoC implementations of all components available, please get in touch
- Finalization of document, shepherd writeup

Backup: BRSKI-PRM – Abstract Protocol Overview

